

# Finite Block Length Analysis on Quantum Coherence Distillation and Incoherent Randomness Extraction

Masahito Hayashi<sup>1</sup>, Fellow, IEEE, Kun Fang<sup>2</sup>, and Kun Wang<sup>3</sup>

**Abstract**—We give the *first* systematic study on the second order asymptotics of the operational task of coherence distillation with and without assistance. In the unassisted setting, we introduce a variant of randomness extraction framework where free incoherent operations are allowed before the incoherent measurement and the randomness extractors. We then show that the maximum number of random bits extractable from a given quantum state is precisely equal to the maximum number of coherent bits distillable from the same state. This relation enables us to derive tight second order expansions of both tasks in the independent and identically distributed setting. Remarkably, the incoherent operation classes that can empower coherence distillation for generic states all admit the same second order expansions, indicating their operational equivalence for coherence distillation in both asymptotic and large block length regimes. We then generalize the above line of research to the assisted setting, arising naturally in bipartite quantum systems where Bob distills coherence from the state at hand, aided by the benevolent Alice possessing the other system. More precisely, we introduce a new assisted incoherent randomness extraction task and establish an exact relation between this task and the assisted coherence distillation. It strengthens the one-shot relation in the unassisted setting and confirms that this cryptographic framework offers a new perspective to the study of quantum coherence distillation. Likewise, this relation yields second order characterizations to the assisted tasks. As by-products, we show the strong converse property of the tasks above from their second order expansions.

Manuscript received March 7, 2020; revised October 14, 2020; accepted February 21, 2021. Date of publication March 4, 2021; date of current version May 20, 2021. The work of Masahito Hayashi was supported in part by the Guangdong Provincial Key Laboratory under Grant 2019B121203002, in part by the Japan Society of the Promotion of Science (JSPS) Grant-in-Aid for Scientific Research (B) under Grant 16KT0017 and for Scientific Research (A) Grant 17H01280, and in part by the Kayamori Foundation of Informational Science Advancement. (Corresponding author: Kun Fang.)

Masahito Hayashi is with the Shenzhen Institute for Quantum Science and Engineering, Southern University of Science and Technology, Shenzhen 518055, China, also with the Guangdong Provincial Key Laboratory of Quantum Science and Engineering, Southern University of Science and Technology, Shenzhen 518055, China, also with the Shenzhen Key Laboratory of Quantum Science and Engineering, Southern University of Science and Technology, Shenzhen 518055, China, and also with the Graduate School of Mathematics, Nagoya University, Nagoya 464-8602, Japan (e-mail: masahito@math.nagoya-u.ac.jp).

Kun Fang was with the Institute for Quantum Computing, University of Waterloo, Waterloo, ON N2L 3G1, Canada. He is now with the Institute for Quantum Computing, Baidu Research, Beijing 100193, China (e-mail: fangfred11@gmail.com).

Kun Wang was with the Shenzhen Institute for Quantum Science and Engineering, Southern University of Science and Technology, Shenzhen 518055, China. He is now with the Institute for Quantum Computing, Baidu Research, Beijing 100193, China.

Communicated by M. M. Wilde, Associate Editor for Quantum Information Theory.

Color versions of one or more figures in this article are available at <https://doi.org/10.1109/TIT.2021.3064009>.

Digital Object Identifier 10.1109/TIT.2021.3064009

**Index Terms**—Coherence distillation, incoherent randomness extraction, second order analysis, strong converse property.

## I. INTRODUCTION

A CENTRAL problem of a general resource theory [1] is *resource distillation*: the process of extracting canonical units of resources from a given quantum state using a choice of free operations. The usual asymptotic approach to studying problems in quantum information theory is to assume that there is an unbounded number of independent and identically distributed (i.i.d.) copies of a source state available and that the error measure asymptotically goes to zero. However, for many practical applications there are natural restrictions on the code length imposed, for example, by limitations on how much quantum information can be processed coherently. Therefore it is crucial to go beyond the asymptotic treatment and understand the intricate tradeoff between different operational parameters of concern.

In general, suppose a quantity of interest is given by  $R(\rho^{\otimes n}, \varepsilon)$  which is a function of the sequence of states  $\{\rho^{\otimes n}\}_{n \in \mathbb{N}}$  and the error threshold  $\varepsilon$ . The typical information-theoretical study focuses on finding the asymptotic rate  $R_1(\rho) := \lim_{\varepsilon \rightarrow 0} \lim_{n \rightarrow \infty} \frac{1}{n} R(\rho^{\otimes n}, \varepsilon)$ . Together with a strong converse property, this is equivalent to expanding  $R(\rho^{\otimes n}, \varepsilon) = nR_1 + o(n)$  where  $R_1$  is called the *first order coefficient*. An estimation to the order  $o(n)$  is usually unsatisfactory in the case with limited resources, motivating us to further investigate the *second order expansion*, a refined estimation of  $R(\rho^{\otimes n}, \varepsilon)$  to the order  $o(\sqrt{n})$ . More precisely, we aim to find an expansion  $R(\rho^{\otimes n}, \varepsilon) = nR_1 + \sqrt{n}R_2 + o(\sqrt{n})$  where  $R_2$  is called the *second order asymptotics*. To achieve this, we shall first consider the *one-shot* scenario where the source is characterized by a single instance of *unstructured* quantum state, and then replace the unstructured state with the i.i.d. state  $\rho^{\otimes n}$  to retrieve the desired second order result.

The significance of second order expansions is multifold. First, second order expansions provide a useful approximation for finite block length  $n$ , refining optimal rates that typically correspond to the first order asymptotics in asymptotic expansions. Second, they determine the convergence rate to the first order asymptotics, analogous to the relation between the Central Limit Theorem and the Berry-Esseen Theorem, as the latter determines the convergence rate in the former. Finally, second order expansions can be used to derive the strong converse property, an information-theoretic property that rules out a possible tradeoff between the transformation error and the rate of resulting resource of a protocol.

In this paper, we focus on the resource theory of quantum coherence [2] and investigate in-depth the second order asymptotics of the coherence distillation task under various settings. In the following two paragraphs, we summarize the state-of-the-art research progress of both the unassisted and assisted coherence distillation tasks, point out the major concerns, and present shortly our strategy to solve these concerns and the obtained results.

*Unassisted coherence distillation and randomness extraction:* Quantum coherence is a physical resource that is essential for various information processing tasks [3]–[9]. A series of efforts have been devoted to building this resource theory in recent years [2], [10]–[13], characterizing in particular the state transformations and operational uses of coherence in fundamental resource manipulation protocols [5], [14]–[19]. The task of coherence distillation in the asymptotic scenario has been first investigated in [14] and has been recently completed in [20]. Despite their theoretical importance, the asymptotic assumptions become unphysical in reality due to our limited access to a finite number of copies of a given state, making it necessary to look at non-asymptotic regimes. The first step in this direction is to consider the one-shot setting that distills coherence from a single instance of the prepared state. Such a scenario has been investigated in [17] and has been mostly completed in [19]. These works estimate the one-shot distillable coherence under different free operations by their corresponding one-shot entropies. The one-shot entropies most accurately describe the operational quantity, yet they tend to be difficult to calculate for large systems, even for the independent and identically distributed (i.i.d.) case. This motivates further investigations of second order expansions.

The usual approach to deriving the second order expansion of an information task is to combine the one-shot entropy bounds on the information quantity and the second order expansion of the corresponding entropies (e.g., [21]–[27]). However, as second order expansions have a strong dependence on the error parameter  $\varepsilon$ , the existing one-shot entropy bounds on distillable coherence [17], [28] are insufficient to get a tight second order expansion. That is, the second order coefficients in the expansion of the one-shot entropy lower and upper bounds are often mismatched. To solve this, we introduce a variant of randomness extraction framework in the context of quantum coherence theory [29], [30] and build an exact connection of this task with coherence distillation. Such a connection provides a new perspective to the study of the distillation process, leading to an almost tight one-shot estimation of distillable coherence. Finally, expanding the one-shot estimation, we obtain the desired second order expansion.

The exact one-shot relation between randomness extraction and coherence distillation builds a bridge between two seemingly different information tasks, providing new perspectives to the study of both problems. Moreover, our second order expansions initiate *the first* large block length analysis in quantum coherence theory, filling an important gap in the literature.

*Assisted coherence distillation and randomness extraction:* Chitambar *et al.* [15] originally proposed the assisted distillation task, arising naturally in bipartite quantum systems in which Bob aims to distill coherent bits from the state at

his hand, aided by the friendly Alice who possesses the other system [31]–[42]. Streltsov *et al.* [43] pushed forward this task by enlarging the set of free operation classes, mimicking the bipartite operation hierarchy well studied in the entanglement resource theory [44]. They coined this the resource theory of coherence in distributed scenarios. Subsequent works have been carried out both on the theoretical [45], [46] and experimental [47]–[49] directions. Recently, Regula *et al.* [50] and Vijayan *et al.* [51] independently studied the one-shot assisted coherence distillation via different approaches, enhancing the asymptotic results [15], [43] to the one-shot realm. However, the existing results are unsatisfactory due to the following reasons. Firstly, they made *a priori* assumption that the bipartite state shared between Alice and Bob is a pure state. It contrasts with the practical scenario that Bob only holds an extension, rather than a purification, of Alice’s state. Secondly, they considered a limited free operation class that Alice performs measurements and Bob performs conditional incoherent operations. It would be meaningful to explore the power of other free classes in the distributed incoherent operation hierarchy. Lastly but most importantly, the previous one-shot bounds cannot lead to tight second order asymptotics.

Our approach towards these concerns is largely inspired by the ideas from the unassisted scenario. More specifically, we propose a variant of randomness extraction framework within the context of distributed quantum coherence theory, which we call the assisted incoherent randomness extraction. We establish an equivalence relation between this task and the assisted coherence distillation in the one-shot regime. It uplifts the relation between coherence distillation and incoherent randomness extraction in the unassisted setting to the assisted scenario. Then, we make use of this relation to draw a complete characterization on these two tasks by proving a one-shot lower bound on the assisted extractable randomness and a one-shot upper bound on the assisted distillable coherence, with matching dependence on the error threshold  $\varepsilon$  in the two bounds. This characterization bestows us with desired second order expansion for both tasks.

*Outline and main contributions:* The main contributions of this paper are listed in Table I for references and can be summarized as follows:

- In Section III, we first propose a variant of randomness extraction framework in the context of quantum coherence theory, and then establish an *exact* relation between the task of randomness extraction and the task of quantum coherence distillation in the one-shot regime. More precisely, we show that the maximum number of secure randomness bits ( $\ell_{\mathcal{O}}^{\varepsilon}$ ) extractable from a given state is equal to the maximum number of coherent bits ( $C_{d,\mathcal{O}}^{\varepsilon}$ ) distillable from the same state. That is, for any quantum state  $\rho$ , error tolerance  $\varepsilon \in [0, 1]$ , it holds  $C_{d,\mathcal{O}}^{\varepsilon}(\rho) = \ell_{\mathcal{O}}^{\varepsilon}(\rho)$ , where free operation class  $\mathcal{O} \in \{\text{MIO}, \text{DIO}, \text{IO}, \text{DIIIO}\}$  whose definitions can be found in Section III-A. We further give one-shot achievable and converse bounds for  $\ell_{\mathcal{O}}^{\varepsilon}$  as well as  $C_{d,\mathcal{O}}^{\varepsilon}$  in terms of hypothesis testing relative entropy, through which we get the second order expansion of our information tasks.

TABLE I

LIST OF RESULTS WITH REFERENCES OBTAINED IN THIS WORK REGARDING BOTH UNASSISTED AND ASSISTED COHERENCE DISTILLATION AND INCOHERENT RANDOMNESS EXTRACTION TASKS. HERE  $\mathcal{O} \in \{\text{MIO, DIO, IO, DIO}\}$  IS A SINGLE PARTITE FREE OPERATION CLASS AND  $\mathcal{F} \in \{\text{LICC, LQICC, SI, SQI, QIP}\}$  IS A BIPARTITE FREE OPERATION CLASS

Assistance	Characterization	Reference
Unassisted case	one-shot equivalence $C_{d,\mathcal{O}}^\varepsilon(\rho_B) = \ell_{\mathcal{O}}^\varepsilon(\rho_B)$	Theorem 1
	second order expansion $C_{d,\mathcal{O}}^\varepsilon(\rho_B^{\otimes n}) = \ell_{\mathcal{O}}^\varepsilon(\rho_B^{\otimes n}) = nD(\rho_B \ \Delta(\rho_B)) + \sqrt{nV(\rho_B \ \Delta(\rho_B))} \Phi^{-1}(\varepsilon^2) + O(\log n)$	Theorem 2
Assisted case	one-shot equivalence $C_{d,\text{QIP}}^\varepsilon(\rho_{AB}) = \ell_{\text{QIP}}^\varepsilon(\rho_{AB})$	Theorem 3
	second order expansion $C_{d,\text{QIP}}^\varepsilon(\rho_{AB}^{\otimes n}), \ell_{\mathcal{F}}^\varepsilon(\rho_{AB}^{\otimes n}) = nD(\rho_{AB} \ \Delta_B(\rho_{AB})) + \sqrt{nV(\rho_{AB} \ \Delta_B(\rho_{AB}))} \Phi^{-1}(\varepsilon^2) + O(\log n)$	Theorem 5

- In Section IV, we first propose the assisted incoherent randomness extraction task within the quantum coherence theory in the distributed scenario, and then set up an equivalence relation between the assisted coherence distillation and the assisted incoherent randomness extraction in the one-shot regime. That is, we show that the maximum number of coherent bits ( $C_{d,\text{QIP}}^\varepsilon$ ) that can be distilled from a bipartite quantum state  $\rho_{AB}$  is equal to the maximum number of secure randomness bits ( $\ell_{\text{QIP}}^\varepsilon$ ) that can be extracted from the same state, where QIP is the set of quantum-incoherent state-preserving operations (cf. Section IV-A). Finally, we prove one-shot achievability bounds for  $\ell_{\mathcal{F}}^\varepsilon$  and one-shot converse bounds for  $C_{d,\mathcal{F}}^\varepsilon$ , where  $\mathcal{F} \in \{\text{LICC, LQICC, SI, SQI, QIP}\}$ , in terms of the hypothesis testing relative entropy. These, together with the established one-shot equivalence relation, yield a one-shot characterization to these two quantities. Invoking the second order expansion of the hypothesis testing relative entropy, we can get the second order expansion of these rates.
- In Section V, we show the strong converse property of all the investigated tasks, coherence distillation, incoherent randomness extraction, and their assisted versions by using the established second order expansions.
- In Section VI, we establish a series of relations among various entropic quantities evaluated on the dephased tripartite state  $\Delta_B(\Psi_{RAB})$ , where  $|\Psi\rangle_{RAB}$  is a purification of  $\rho_{AB}$  and  $\Delta_B$  is a completely dephasing channel on system  $B$ . These relations are essential to our second order analysis and may find applications in other quantum information processing tasks.
- In Appendix B, we conceive an alternative formulation of the assisted incoherent randomness extraction. The advantage of this alternative is that we can establish an equivalent relation between the assisted coherence distillation and the alternative assisted incoherent randomness extraction for *all* free operation classes under consideration. However, a second order expansion for this alternative task is still missing.

## II. PRELIMINARIES

In this section, we define several quantities and set the notation that will be used throughout this paper. We label different physical systems by capital Latin letters (e.g.  $A, B, C, L$ ). We often use these labels as subscripts to guide the reader by indicating which system a mathematical object belongs to. We drop the subscripts when they are evident in the context of an expression (or if we are not talking about a specific system). The corresponding Hilbert spaces of these physical systems are denoted as  $\mathcal{H}_A, \mathcal{H}_B, \mathcal{H}_C, \mathcal{H}_L$ . The corresponding alphabet sets are denoted by the same letters in math font (e.g.,  $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{L}$ ). For example,  $\mathcal{A} := \{1, 2, \dots, |A|\}$  where  $|A|$  is the dimension of Hilbert space  $\mathcal{H}_A$ . Let  $\{|a\rangle\}_{a \in \mathcal{A}}$  be the computational basis on Hilbert space  $\mathcal{H}_A$ . The set of positive semidefinite operators on  $\mathcal{H}_A$  is denoted as  $\mathcal{P}(A)$ . The set of quantum states, which are positive semidefinite operators with unit trace, on  $\mathcal{H}_A$  is denoted as  $\mathcal{S}(A)$ . Denote the completely mixed state on  $\mathcal{H}_A$  as  $\pi_A$ . The identity operator and the identity map are denoted as  $\mathbb{1}$  and  $\text{id}$ , respectively. A quantum operation  $\Lambda_{A \rightarrow C}$  is a completely positive trace-preserving (CPTP) map from  $\mathcal{S}(A)$  to  $\mathcal{S}(C)$ . All logarithms in this work are taken base two.

For any  $\rho, \sigma \in \mathcal{P}$ , the purified distance  $P$  is defined in terms of the generalized quantum fidelity  $F$  as  $P(\rho, \sigma) := \frac{\sqrt{1 - F(\rho, \sigma)^2}}{\|\sqrt{\rho}\sqrt{\sigma}\|_1 + \sqrt{(1 - \text{Tr } \rho)(1 - \text{Tr } \sigma)}}$  [52]. For any  $\rho \in \mathcal{S}$  and  $\sigma \in \mathcal{P}$ , their quantum hypothesis testing relative entropy is defined as  $D_H^\varepsilon(\rho \|\sigma) := -\log \min\{\text{Tr } M\sigma : \text{Tr } M\rho \geq 1 - \varepsilon, 0 \leq M \leq \mathbb{1}\}$  [53]–[55]. The smooth max-relative entropy is defined as  $D_{\max}^\varepsilon(\rho \|\sigma) := \min_{P(\tilde{\rho}, \rho) \leq \varepsilon} \inf\{\lambda : \tilde{\rho} \leq 2^\lambda \sigma\}$  [56]. The second order expansions of quantum hypothesis testing relative entropy [22], [23] and smooth max-relative entropy [22] are, respectively, given by

$$\begin{aligned}
 D_H^\varepsilon(\rho^{\otimes n} \|\sigma^{\otimes n}) &= nD(\rho \|\sigma) + \sqrt{nV(\rho \|\sigma)} \Phi^{-1}(\varepsilon) + O(\log n), \quad (1) \\
 D_{\max}^\varepsilon(\rho^{\otimes n} \|\sigma^{\otimes n}) &= nD(\rho \|\sigma) - \sqrt{nV(\rho \|\sigma)} \Phi^{-1}(\varepsilon^2) + O(\log n), \quad (2)
 \end{aligned}$$

where  $D(\rho\|\sigma) := \text{Tr}[\rho(\log \rho - \log \sigma)]$  is the quantum relative entropy,  $V(\rho\|\sigma) := \text{Tr}[\rho(\log \rho - \log \sigma)^2] - D(\rho\|\sigma)^2$  is the quantum information variance and  $\Phi^{-1}$  is the inverse of the cumulative distribution function of a standard normal random variable.

For any  $\sigma \in \mathcal{P}$ , we denote the number of distinct non-zero eigenvalues of  $\sigma$  by  $\nu(\sigma)$ . Let  $\lambda_{\max}$  and  $\lambda_{\min}$  be the maximum and minimum non-zero eigenvalues of  $\sigma$ , respectively. Set  $\lambda(\sigma) := \log \lambda_{\max}(\sigma) - \log \lambda_{\min}(\sigma)$ . The following  $\theta$  function is commonly used in one-shot information quantities:

$$\theta(\sigma) := \min\{2\lceil\lambda(\sigma)\rceil, \nu(\sigma)\}. \quad (3)$$

### III. QUANTUM COHERENCE DISTILLATION AND INCOHERENT RANDOMNESS EXTRACTION

In this section, we first review the resource theory of quantum coherence and the operational task of quantum coherence distillation. We then introduce a variant of the randomness extraction framework in the context of quantum coherence theory.

#### A. Resource Theory of Quantum Coherence

The resource theory of coherence consists of the following ingredients [13]: the set of *free states* and the set of *free operations*, that is, a set of quantum operations that do not generate coherence. The free states, so-called incoherent states, are the quantum states which are diagonal in a given reference orthonormal basis  $\{|b\rangle\}_{b \in \mathcal{B}}$ . We will use  $\Delta_B(\cdot) := \sum_{b \in \mathcal{B}} |b\rangle\langle b| \cdot |b\rangle\langle b|$  to denote the diagonal map (completely dephasing channel) in this basis.<sup>1</sup> Then the set of incoherent states is denoted as  $\mathcal{I}(B) := \{\rho \in \mathcal{S}(B) : \rho = \Delta_B(\rho)\}$ . For convenience, we will also use the cone of diagonal positive semidefinite matrices, which is denoted as  $\mathcal{I}^{**}(B) := \{X \in \mathcal{P}(B) : X = \Delta_B(X)\}$ . The maximal resource state on  $\mathcal{H}_B$  is the *maximally coherent state (MCS)*  $|\Psi_B\rangle := 1/\sqrt{|\mathcal{B}|} \sum_{b=1}^{|\mathcal{B}|} |b\rangle$  with dimension  $|\mathcal{B}|$ . Denote its density operator as  $\Psi_B := |\Psi_B\rangle\langle\Psi_B|$ . The resource theory of coherence is known not to admit a unique physically-motivated choice of allowed free operations [2], [14], [57]–[59]. The relevant choices of free operations that we will focus on are: *maximally incoherent operations (MIO)* [10], defined to be all operations  $\Lambda$  such that  $\Lambda(\rho) \in \mathcal{I}$  for every  $\rho \in \mathcal{I}$ ; *dephasing-covariant incoherent operations (DIO)* [57], [58], which are maps  $\Lambda$  such that  $\Delta \circ \Lambda = \Lambda \circ \Delta$ ; *incoherent operations (IO)* [13], which admit a set of incoherent Kraus operators  $\{K_l\}$  such that  $K_l \rho K_l^\dagger \in \mathcal{I}^{**}$  for all  $l$  and  $\rho \in \mathcal{I}$ ; the intersection of IO and DIO is denoted as  $\text{DIIO} := \text{DIO} \cap \text{IO}$  [28]. Another two classes of free operations commonly studied are *strictly incoherent operations (SIO)* [14] and *physically incoherent operations (PIO)* [57]. We do not investigate further details of SIO and PIO, as it has been recently shown that quantum coherence is generically undistillable under these two classes [20], [60]. Finally, the inclusion relations between free operation classes can be summarized as  $\text{DIIO} \subsetneq \text{IO} \subsetneq \text{MIO}$ ,

<sup>1</sup>In this section, we assume that Bob instead of the commonly used Alice is the main party of all the operations, thus the symbol of our notations starts from the letter  $B$ . We do so to keep consistent with the later assisted scenario in which Alice serves as assistance.

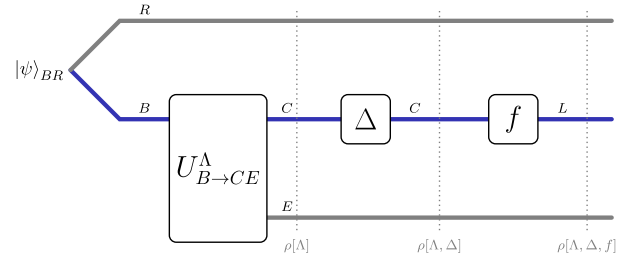


Fig. 1. Schematic diagram of an incoherent randomness extraction protocol given by  $(\Lambda, \Delta, f)$ .  $|\psi\rangle_{BR}$  is a purification of  $\rho_B$ .  $U_{B \to CE}^\Lambda$  is the Stinespring representation of  $\Lambda_{B \to C} \in \mathcal{O}$ .  $\Delta$  is a completely dephasing channel and  $f$  is a hash function from alphabet  $\mathcal{C}$  to  $\mathcal{L}$ .  $\rho[\Lambda]$ ,  $\rho[\Lambda, \Delta]$  and  $\rho[\Lambda, \Delta, f]$  are respectively the output states in each step of the protocol. The systems in blue belong to Bob and the systems in gray belong to Eve.

$\text{DIIO} \subsetneq \text{DIO} \subsetneq \text{MIO}$ , while IO and DIO are not contained by each other.

#### B. Framework of Quantum Coherence Distillation

The task of *coherence distillation* aims to transform a given quantum state  $\rho_B$  to a maximally coherent state  $\Psi_C$  such that the obtained maximally coherent state has dimension as large as possible and that the transformation error is within a given threshold. More formally, for any free operation class  $\mathcal{O}$ , any given state  $\rho_B \in \mathcal{S}(B)$  and error threshold  $\varepsilon \in [0, 1]$ , the *one-shot distillable coherence* is defined as

$$C_{d, \mathcal{O}}^\varepsilon(\rho_B) := \max_{\Lambda \in \mathcal{O}} \{\log |C| : P(\Lambda_{B \to C}(\rho_B), \Psi_C) \leq \varepsilon\}. \quad (4)$$

Note that some previous works (e.g., [17], [18], [28]) estimate the performance of distillation by the error criterion  $P(\Lambda_{B \to C}(\rho_B), \Psi_C) \leq \sqrt{\varepsilon}$ . Here we use the definition in (4) for convenience.

#### C. Framework of Incoherent Randomness Extraction

The task of *incoherent randomness extraction* aims to obtain as many random bits as possible in Bob's laboratory that is secure from the possible adversary Eve. A general *incoherent randomness extraction protocol* is characterized by a triplet  $(\Lambda, \Delta, f)$ , where  $\Lambda$  is an incoherent operation in a certain class,  $\Delta$  is a completely dephasing channel and  $f$  is a hash function. A detailed procedure of randomness extraction by  $(\Lambda, \Delta, f)$  is depicted in Figure 1. Here, we assume that Eve has unlimited power in her system and all the information of Eve about Bob's systems is encoded in a purification. That is, for any given quantum state  $\rho_B$  held by Bob, we denote its purification as<sup>2</sup>

$$|\psi\rangle_{BR} := \sum_{b \in \mathcal{B}} \sqrt{p_b} |b\rangle_B |\psi_b\rangle_R \text{ with } \text{Tr}_R |\psi\rangle\langle\psi|_{BR} = \rho_B, \quad (5)$$

where  $R$  is the reference system held by Eve. Then the extraction protocol follows three steps:

- 1) Bob first performs a free operation  $\Lambda_{B \to C} \in \mathcal{O}$  on his part of the system. If he uses a quantum operation whose final state is always a specific incoherent state, say the maximally mixed state  $\pi_C$ , the resulting conditional entropy equals  $\log |C|$ , which increases unlimitedly as

<sup>2</sup>Note that  $|\psi_b\rangle$  are not necessarily orthogonal to each other.

$|C|$  increases. To avoid such a trivial advantage for Bob, similar to the study of quantum key distribution [61]–[63] and private capacity in quantum Shannon theory [64], we assume that the environment system  $\mathcal{H}_E$  of the free operation  $\Lambda$  is also controlled by Eve. This is because it is not easy to exclude the possibility that Eve accesses a system that interacts with Bob's operation. Hence Eve has control over two systems  $\mathcal{H}_R$  and  $\mathcal{H}_E$  in total. To cover such a worst scenario, we consider the Stinespring representation  $U^\Lambda$  of  $\Lambda$ , where  $U^\Lambda$  is the isometry from  $\mathcal{H}_B$  to  $\mathcal{H}_C \otimes \mathcal{H}_E$ .<sup>3</sup> After the action of  $\Lambda$ , the total output state is a pure state

$$\rho[\Lambda]_{CER} := U^\Lambda |\psi\rangle\langle\psi| (U^\Lambda)^\dagger. \quad (6)$$

- 2) Next, Bob performs an incoherent measurement, with respect to the computational basis, on his part of the state. The output state is then given by

$$\rho[\Lambda, \Delta]_{CER} := \Delta_C(\rho[\Lambda]_{CER}). \quad (7)$$

- 3) Finally, a hash function  $f$  is applied on his part of the system to extract the randomness that is secure from Eve. For any deterministic function  $f: \mathcal{C} \rightarrow \mathcal{L}$ , and any classical-quantum (CQ) state  $\rho_{CR} = \sum_{c \in \mathcal{C}} t_c |c\rangle\langle c|_C \otimes \rho_{R|c}$ , denote  $\rho_{f(C)R} := \sum_{c \in \mathcal{C}} t_c |f(c)\rangle\langle f(c)|_L \otimes \rho_{R|c}$ . Then the output state in the final step is given by

$$\rho[\Lambda, \Delta, f]_{LER} := \rho[\Lambda, \Delta]_{f(C)ER}. \quad (8)$$

To quantify the security of randomness in a quantum state  $\rho_{BR}$  with respect to the reference system  $\mathcal{H}_R$ , we employ the following measure:

$$d_{sec}(\rho_{BR}|R) := \min_{\sigma_R \in \mathcal{S}(R)} P(\rho_{BR}, \pi_B \otimes \sigma_R). \quad (9)$$

This measure quantifies the closeness of a given quantum state  $\rho_{BR}$  to an ideal state  $\pi_B$  which contains perfect randomness and is decoupled from the reference system  $\mathcal{H}_R$ . Based on this security measure, the *one-shot extractable randomness under given free operation*  $\Lambda \in \mathcal{O}$  is defined as

$$\ell_\Lambda^\varepsilon(\rho_B) := \max_f \{ \log |L| : d_{sec}(\rho[\Lambda, \Delta, f]_{LER}|ER) \leq \varepsilon \}. \quad (10)$$

The *one-shot extractable randomness under free operation class*  $\mathcal{O}$  is then defined by optimizing all possible choices of operation  $\Lambda$  in  $\mathcal{O}$ :

$$\ell_{\mathcal{O}}^\varepsilon(\rho_B) := \max_{\Lambda \in \mathcal{O}} \ell_\Lambda^\varepsilon(\rho_B). \quad (11)$$

Note that the identity map  $\text{id}$  is always free in coherence theory. Thus  $(\text{id}, \Delta, f)$  is a valid incoherent randomness extraction protocol for any  $f$ , which was studied in [22, Section III]. That is, Bob directly performs an incoherent measurement  $\Delta$  on his given state  $\rho_B$ . In this case, the environment system  $\mathcal{H}_E$  reduces to trivial and system  $\mathcal{H}_C = \mathcal{H}_B$ . It has been shown in [22, Theorem 8] that for any  $\eta \in (0, \varepsilon]$ ,

$$H_{\min}^{\varepsilon-\eta}(B|R)_\sigma + 4 \log \eta - 3 \leq \ell_{\text{id}}^\varepsilon(\rho_B) \leq H_{\min}^\varepsilon(B|R)_\sigma, \quad (12)$$

<sup>3</sup>Note that a free operation does not necessarily admit a free dilation [57]. Thus  $U^\Lambda$  is not necessarily incoherent though  $\Lambda$  is free.

where

$$H_{\min}^\varepsilon(B|R)_\rho := \max_{\omega_R \in \mathcal{S}(R)} -D_{\max}^\varepsilon(\rho_{BR} \| \mathbb{1}_B \otimes \omega_R) \quad (13)$$

is the conditional min-entropy and  $\sigma_{BR} := \rho[\text{id}, \Delta]$  is the dephased classical-quantum state in the protocol.

*Remark 1:* On the one hand, the randomness extraction protocol without using incoherent operations (e.g., the one considered in [28, Figure 1.(b)]) is too restrictive, as such a framework does not make good use of free resources at hand. On the other hand, an extraction protocol that does not consider Eve's attack on the free operation  $\Lambda$  is too trivial because Bob can generate an arbitrary amount of randomness by using a free replacer channel  $\Lambda(\cdot) = \pi_C$ . Hence, the setup in Figure 1 contributes to a reasonable randomness extraction framework in the context of quantum coherence theory.

*Remark 2:* Note that performing incoherent unitary operations in the first step does not make any difference with the protocol by identity map  $\text{id}$ . This justifies our consideration of general incoherent operations. More precisely, for any incoherent unitary  $U$ , it holds  $\ell_{\text{id}}^\varepsilon(\rho_B) = \ell_U^\varepsilon(\rho_B)$  with  $\mathcal{U}(\cdot) := U(\cdot)U^\dagger$ . To see this, recall that any incoherent unitary on  $\mathcal{H}_B$  can be written as  $U_B = \sum_{b \in \mathcal{B}} e^{i\theta_b} |g(b)\rangle\langle b|$  with a permutation  $g$  and phase factors  $e^{i\theta_b}$  [2, Section II.A.2]. Then a direct calculation gives that  $\rho[\mathcal{U}, \Delta, f] = \sum_{b \in \mathcal{B}} p_b |f(g(b))\rangle\langle f(g(b))| \otimes |\psi_b\rangle\langle\psi_b| = \rho[\text{id}, \Delta, f \circ g]$ , implying the equivalence of extraction protocols  $(\mathcal{U}, \Delta, f)$  and  $(\text{id}, \Delta, f \circ g)$ . Then  $\ell_{\text{id}}^\varepsilon(\rho_B) = \ell_U^\varepsilon(\rho_B)$  follows by definition.

*Remark 3:* The randomness extraction framework proposed here is also closely related to the one in [30]. But we should note the following subtle differences: (i) the independence of the resulting randomness is quantified using the trace distance in [30] instead of the purified distance we use in (9). Though the trace distance can give us the nice property of universal compositability (see [65]), the choice of purified distance in (9) is crucial for obtaining the exact relation between coherence distillation and randomness extraction in the next section, which then becomes a key ingredient to proving the second order expansions; (ii) while the paper [30] discusses the large block length regime, its analysis focuses the exponential decreasing rate for the amount of the leaked information  $\varepsilon$ , but we will put more focus on the rate of extractable randomness in the one-shot and large block length regime with constant  $\varepsilon$ .

The references [29] and [30, Section VI] also address the randomness extraction via incoherent operations but with additional constraints on Eve, which are different from our setting here.

#### D. Relation Between Coherence Distillation and Randomness Extraction

In this section, we present an exact connection between incoherent randomness extraction and coherence distillation, the proof of which showcases a nice one-to-one correspondence between protocols in these tasks.

We first present a method of constructing a coherence distillation protocol from a given randomness extraction protocol with the same performance, which will be used in showing the one-shot connection. We note that this method has essentially

been proposed in the proof of [28, Theorem 4], using the trace distance in the security measure. Whereas in our formulation, the purified distance is preferred and is crucial in establishing tight second order asymptotics.

*Proposition 1:* For any quantum state  $\rho_B \in \mathcal{S}(B)$ , error tolerance  $\varepsilon \in [0, 1]$  and incoherent randomness extraction protocol  $(\text{id}, \Delta, f)$  such that  $d_{\text{sec}}(\rho[\text{id}, \Delta, f]_{LR}|R) \leq \varepsilon$ , there exists a quantum operation  $\Gamma : \mathcal{S}(B) \rightarrow \mathcal{S}(L)$  such that  $\Gamma \in \text{DIIO}$  and  $P(\Gamma_{B \rightarrow L}(\rho_B), \Psi_L) \leq \varepsilon$ .

The proof can be found in Appendix A.

*Theorem 1 (Exact One-Shot Connection):* For any quantum state  $\rho_B \in \mathcal{S}(B)$ , error tolerance  $\varepsilon \in [0, 1]$  and free operation class  $\mathcal{O} \in \{\text{MIO}, \text{DIO}, \text{IO}, \text{DIIO}\}$ , the following equation holds

$$C_{d,\mathcal{O}}^\varepsilon(\rho_B) = \ell_{\mathcal{O}}^\varepsilon(\rho_B). \quad (14)$$

*Remark 4:* Recall that there is an exact characterization of one-shot distillable coherence under MIO and DIO operations [17, Proposition 2]. Together with the above (14), we have the following chain of equalities:

$$\begin{aligned} C_{d,\text{MIO}}^\varepsilon(\rho_B) &= C_{d,\text{DIO}}^\varepsilon(\rho_B) = \ell_{\text{MIO}}^\varepsilon(\rho_B) = \ell_{\text{DIO}}^\varepsilon(\rho_B) \\ &= \min_{\substack{X=\Delta(X) \\ \text{Tr } X=1}} D_H^\varepsilon(\rho_B \| X) - \delta, \end{aligned} \quad (15)$$

where the minimum is taken over all Hermitian operators  $X$  on  $\mathcal{H}_B$  satisfying the conditions and  $\delta \geq 0$  is the least number such that the solution corresponds to the logarithm of an integer.

*Remark 5:* A one-shot relation between distillable coherence and extractable randomness has appeared in [28, Equation (80)]. Unlike the precise equation in (14), the relation in [28] is given in the form of one-shot lower and upper bounds with unmatched error dependence and additional correction terms. However, the clean form in (14) plays a pivotal role in deriving the second order expansions where the error dependence matters.

*Proof of Theorem 1:* We first show the direction  $\ell_{\mathcal{O}}^\varepsilon(\rho_B) \geq C_{d,\mathcal{O}}^\varepsilon(\rho_B)$ . Denote  $C_{d,\mathcal{O}}^\varepsilon(\rho_B) = \log |C|$  and suppose that this rate is achieved by a free operation  $\Lambda : \mathcal{S}(B) \rightarrow \mathcal{S}(C)$  such that  $P(\Lambda(\rho_B), \Psi_C) \leq \varepsilon$ . Consider a randomness extraction protocol  $(\Lambda, \Delta, \text{id})$ . Note that  $\rho[\Lambda]_{\text{CER}}$  is a purification of  $\Lambda(\rho_B)$ . By Uhlmann's theorem [66] there exists an extension of  $\Psi_C$ , denoted as  $\Psi_C \otimes \sigma_{ER}^*$ , such that  $P(\Lambda(\rho_B), \Psi_C) = P(\rho[\Lambda]_{\text{CER}}, \Psi_C \otimes \sigma_{ER}^*)$ . Then we have

$$d_{\text{sec}}(\rho[\Lambda, \Delta, \text{id}]_{\text{CER}}|ER) \quad (16)$$

$$= \min_{\sigma_{ER} \in \mathcal{S}(ER)} P(\Delta_C(\rho[\Lambda]_{\text{CER}}), \pi_C \otimes \sigma_{ER}) \quad (17)$$

$$\leq P(\Delta_C(\rho[\Lambda]_{\text{CER}}), \pi_C \otimes \sigma_{ER}^*) \quad (18)$$

$$= P(\Delta_C(\rho[\Lambda]_{\text{CER}}), \Delta_C(\Psi_C \otimes \sigma_{ER}^*)) \quad (19)$$

$$\leq P(\rho[\Lambda]_{\text{CER}}, \Psi_C \otimes \sigma_{ER}^*) \quad (20)$$

$$= P(\Lambda(\rho_B), \Psi_C) \quad (21)$$

$$\leq \varepsilon, \quad (22)$$

where the second equality follows by  $\Delta_C(\Psi_C) = \pi_C$ , the second inequality follows by the data-processing inequality of purified distance, the third equality follows from the

assumption of  $\sigma_{ER}^*$ . Thus we know that  $\log |C|$  is a achievable randomness extraction rate, which implies  $\ell_{\mathcal{O}}^\varepsilon(\rho_B) \geq \log |C| = C_{d,\mathcal{O}}^\varepsilon(\rho_B)$ .

For the other direction, we denote  $\ell_{\mathcal{O}}^\varepsilon(\rho_B) = \log |L|$  and suppose that this rate is achieved by an extraction protocol  $(\Lambda, \Delta, f)$  with  $\Lambda \in \mathcal{O}$ . Observe that applying the protocol  $(\Lambda, \Delta, f)$  on quantum state  $\rho_B$  is the same as applying a protocol  $(\text{id}, \Delta, f)$  on  $\Lambda(\rho_B)$  with purification  $\rho[\Lambda]_{\text{CER}}$  and reference system  $ER$ . By Proposition 1 there exists a quantum operation  $\Gamma : \mathcal{S}(C) \rightarrow \mathcal{S}(L)$  such that  $\Gamma \in \text{DIIO}$  and  $P(\Gamma(\Lambda(\rho_B)), \Psi_L) \leq \varepsilon$ . Since  $\Gamma \in \text{DIIO} \subseteq \mathcal{O}$  and  $\Lambda \in \mathcal{O}$ , we have  $\Gamma \circ \Lambda \in \mathcal{O}$  and this operation achieves the distillation rate  $\log |L|$ . This implies  $C_{d,\mathcal{O}}^\varepsilon(\rho_B) \geq \log |L| = \ell_{\mathcal{O}}^\varepsilon(\rho_B)$  and completes the proof. ■

## E. Second Order Analysis

In this section, we discuss the second order expansions of distillable coherence and extractable randomness. For this, we first show a one-shot characterization of distillable coherence by the hypothesis testing relative entropy.

*Proposition 2 (One-Shot Characterization):* For any quantum state  $\rho_B \in \mathcal{S}(B)$ , free operation class  $\mathcal{O} \in \{\text{MIO}, \text{DIO}, \text{IO}, \text{DIIO}\}$ , error tolerance  $\varepsilon \in (0, 1)$  and  $0 < \eta < \varepsilon$ ,  $0 < \delta < \min\{(\varepsilon - \eta)^2/3, 1 - (\varepsilon - \eta)^2\}$ , it holds

$$\begin{aligned} D_H^{(\varepsilon - \eta)^2 - 2\delta}(\rho_B \| \Delta(\rho_B)) - c(\rho_B, \varepsilon, \delta, \eta) \\ \leq C_{d,\mathcal{O}}^\varepsilon(\rho_B) \leq D_H^{\varepsilon^2}(\rho_B \| \Delta(\rho_B)), \end{aligned} \quad (23)$$

where  $c(\rho_B, \varepsilon, \delta, \eta) = \log \theta(\rho_B) + \log \theta(\Delta(\rho_B)) + \log((\varepsilon - \eta)^2 - \delta) - \log(\delta^5 \eta^4 (\varepsilon - \eta)^2 (1 - (\varepsilon - \eta)^2 + \delta)) + 11$ .

*Proof:* The upper bound follows from a known result in [17, Proposition 2] (see also (15)). Choosing a feasible solution  $X$  as  $\Delta(\rho)$ , we have  $C_{d,\mathcal{O}}^\varepsilon(\rho_B) \leq C_{d,\text{MIO}}^\varepsilon(\rho_B) \leq D_H^{\varepsilon^2}(\rho_B \| \Delta(\rho_B))$  where the first inequality follows by the fact that  $\mathcal{O} \subseteq \text{MIO}$ . As for the lower bound, we have  $C_{d,\mathcal{O}}^\varepsilon(\rho_B) = \ell_{\mathcal{O}}^\varepsilon(\rho_B) \geq \ell_{\text{id}}^\varepsilon(\rho_B) \geq H_{\text{min}}^{\varepsilon - \eta}(B|R)_\sigma + 4 \log \eta - 3$  where the first equality follows from Theorem 1, the first inequality follows since  $\text{id} \in \mathcal{O}$ , the second inequality follows from (12). By (101) of Proposition 4 we can further lower bound the conditional min-entropy by the hypothesis testing relative entropy. This gives us the one-shot lower bound stated in (23). ■

Now we are ready to present our main result in this section.

*Theorem 2 (Second Order Expansion):* For any quantum state  $\rho_B \in \mathcal{S}(B)$ , error tolerance  $\varepsilon \in (0, 1)$  and free operation class  $\mathcal{O} \in \{\text{MIO}, \text{DIO}, \text{IO}, \text{DIIO}\}$ , the following second order expansions hold

$$\begin{aligned} C_{d,\mathcal{O}}^\varepsilon(\rho_B^{\otimes n}) &= \ell_{\mathcal{O}}^\varepsilon(\rho_B^{\otimes n}) = nD(\rho_B \| \Delta(\rho_B)) \\ &\quad + \sqrt{nV(\rho_B \| \Delta(\rho_B))} \Phi^{-1}(\varepsilon^2) + O(\log n), \end{aligned} \quad (24)$$

where  $\Phi^{-1}$  denotes the inverse of the cumulative distribution function of a standard normal random variable.

*Proof:* The first equality follows from the one-shot relation in Theorem 1. We now prove that the second order expansion holds for  $C_{d,\mathcal{O}}^\varepsilon(\rho_B^{\otimes n})$ . This can be seen as a direct consequence of expanding the one-shot characterization in

Proposition 2. Given the i.i.d. state  $\rho_B^{\otimes n}$ , we have

$$C_{d,\mathcal{O}}^\varepsilon(\rho_B^{\otimes n}) \leq D_H^{\varepsilon^2}(\rho_B^{\otimes n} \|\Delta(\rho_B)^{\otimes n}). \quad (25)$$

Expanding the r.h.s. via formula (1) we have the second order upper bound. On the other hand, we have

$$C_{d,\mathcal{O}}^\varepsilon(\rho_B^{\otimes n}) \geq D_H^{(\varepsilon-\eta)^2-2\delta}(\rho_B^{\otimes n} \|\Delta(\rho_B)^{\otimes n}) - c(\rho_B^{\otimes n}, \varepsilon, \delta, \eta). \quad (26)$$

By definition (3),  $\theta(\sigma^{\otimes n}) \leq 2\lceil \lambda(\sigma^{\otimes n}) \rceil = 2\lceil n\lambda(\sigma) \rceil$  which scales at most linearly in  $n$ . Choosing  $\eta$  and  $\delta$  proportional to  $1/\sqrt{n}$ , we know that the correction term  $c(\rho_B^{\otimes n}, \varepsilon, \delta, \eta) \in O(\log n)$  and  $\Phi^{-1}((\varepsilon - \eta)^2 - 2\delta) = \Phi^{-1}(\varepsilon^2) + O(1/\sqrt{n})$ . Thus expanding the r.h.s. of (26) via formula (1) leads to the second order lower bound which matches exactly with the upper bound. ■

*Remark 6:* From Proposition 4 in Section VI, the first and second order asymptotics can also be written as conditional entropy  $H(B|R)_{\sigma_{BR}}$  and conditional information variance  $V(B|R)_{\sigma_{BR}}$  respectively, where  $\sigma_{BR} = \rho[\text{id}, \Delta]$  is the dephased classical-quantum state from the randomness extraction protocol.

*Remark 7:* Comparing the second order expansion of  $\ell_{\text{id}}^\varepsilon(\rho_B^{\otimes n})$  in [22, Corollary 16] and the result above, we can conclude that a general incoherent randomness extraction protocol  $(\Lambda, \Delta, f)$  has no advantage over the protocol  $(\text{id}, \Delta, f)$  in the sense that they lead to the same first order asymptotics [30] and the second order asymptotics of extractable randomness. However, this does not rule out a possible advantage in the third or higher order terms.

*Remark 8:* The distillable coherence under operation classes MIO/DIO/IO/DIIO not only have the same first order asymptotics as observed in [14], [17], [28] but also have the same second order asymptotics, indicating that they are equivalently powerful for coherence distillation in the large block length regime. The same argument goes to the incoherent randomness extraction.

*Remark 9:* For any quantum state  $\rho_B = \sum_{i,j} \rho_{ij} |i\rangle\langle j|_B$  written in the computational basis, we can assign it to a bipartite maximally correlated state  $\rho_{\text{mc}} := \sum_{i,j} \rho_{ij} |i\rangle\langle j|_A \otimes |i\rangle\langle j|_B$ . The second order expansion of distillable entanglement of  $\rho_{\text{mc}}^{\otimes n}$  under local operations and classical communication (LOCC) is also given by  $nD(\rho \|\Delta(\rho)) + \sqrt{nV(\rho \|\Delta(\rho))} \Phi^{-1}(\varepsilon^2) + O(\log n)$  [26, Proposition 10]. Together with the result in Theorem 2, the coincidence of these second order expansions leads to a new evidence to the long-standing conjecture (see e.g. [2, Section II.D]) that any incoherent operation acting on a state  $\rho_B$  is equivalent to a LOCC operation acting on the associated maximally correlated state  $\rho_{\text{mc}}$ .

*Remark 10:* Compared with the one-shot estimation in [28, Equations (37,46,47)], we can verify that their upper and lower bounds on the one-shot distillable coherence agree in the first order term but *disagree* in the second order term. In particular, the dependence on  $\varepsilon$  is qualitatively different in their upper and lower bounds. Thus, one could certainly argue that the bounds in [28] are not as tight as they should be in the asymptotic limit.

#### IV. ASSISTED COHERENCE DISTILLATION AND ASSISTED INCOHERENT RANDOMNESS EXTRACTION

In this section, we first introduce the resource theory of quantum coherence in the distributed scenario and then formally define two different resource processing tasks with assistance from the environment within this resource theory. The first is the assisted quantum coherence distillation initially investigated in [15], [43]. The second is a variant of the randomness extraction task adapted into the distributed scenario, which plays a crucial role in establishing the second order characterization of the former task.

##### A. Resource Theory of Quantum Coherence in Distributed Scenarios

Motivated by the local operations and classical communication known from entanglement theory [44], Chitambar *et al.* [15] seminaly introduced the framework of local incoherent operations and classical communication (LICC) in the distributed resource theory of quantum coherence, which was later further explored by Streltsov *et al.* [43]. In this scenario, there are two separate parties, Alice and Bob, that are connected via a classical channel and restricted to performing local incoherent operations. We think of Alice as an assistant who helps Bob to manipulate coherence. Here we briefly summarize several sets of free bipartite quantum operations widely studied in the distributed resource theory of coherence and refer the interested readers to [43], [67] for more details:

- LICC: the set of *local incoherent operations and classical communication* [15]. That is, Alice and Bob perform local incoherent operations and share their outcomes via a classical channel. Throughout this work, we assume without loss of generality that the free local operations are chosen to be MIO<sup>4</sup>;
- LQICC: the set of *local quantum-incoherent operations and classical communication* [15]. That is, Alice can adopt arbitrary quantum operations while Bob is restricted to quantum incoherent operations, and they share the outcomes via a classical channel;
- SI: the set of *separable incoherent operations* [43]:

$$\Lambda_{AB \rightarrow A'B'}(\cdot) := \sum_i (A_i \otimes B_i)(\cdot)(A_i \otimes B_i)^\dagger, \quad (27)$$

where both  $A_i$  and  $B_i$  are incoherent Kraus operators satisfying  $\sum_i A_i^\dagger A_i \otimes B_i^\dagger B_i = \mathbb{1}_{AB}$ ;

- SQI: the set of *separable quantum-incoherent operations* [43] of the form (27), where  $B_i$  are incoherent Kraus operators satisfying  $\sum_i A_i^\dagger A_i \otimes B_i^\dagger B_i = \mathbb{1}_{AB}$ .

The two free classes LQICC and SQI lead to the same set of free states, which is called the *quantum-incoherent states* [15], [43] (system  $A$  is quantum and system  $B$  is incoherent) and

<sup>4</sup>One may choose other sets of local incoherent operations, say SIO or IO, but all of these free local operations lead to the same result in the distributed setting [50, Section III]. We choose MIO since QIP reduces to MIO in the single partite scenario.

bears the form

$$\mathcal{QI}(A:B) := \left\{ \sigma_{AB} = \sum_{b \in \mathcal{B}} p_b \sigma_A^b \otimes |b\rangle\langle b|_B : \right. \\ \left. p_b \geq 0, \sum_{b \in \mathcal{B}} p_b = 1, \sigma_A^b \in \mathcal{S}(A) \right\}. \quad (28)$$

This motivates us to define the maximal set of free operations that preserve  $\mathcal{QI}$ , the set of *quantum-incoherent state preserving operations* QIP [67]:

$$\text{QIP} := \left\{ \Lambda_{AB \rightarrow A'B'} \text{ a quantum operation:} \right. \\ \left. \forall \sigma_{AB} \in \mathcal{QI}, \Lambda_{AB \rightarrow A'B'}(\sigma_{AB}) \in \mathcal{QI} \right\}. \quad (29)$$

By definition the following inclusion relations hold:

$$\text{LICC} \subseteq \text{LQICC} \subseteq \text{SQI} \subseteq \text{QIP}, \\ \text{LICC} \subseteq \text{SI} \subseteq \text{SQI} \subseteq \text{QIP}. \quad (30)$$

In the following, we assume  $\mathcal{F}$  be some chosen free *bipartite* operation class in  $\{\text{LICC}, \text{LQICC}, \text{SI}, \text{SQI}, \text{QIP}\}$ , which is different from the free class  $\mathcal{O} \in \{\text{MIO}, \text{DIO}, \text{IO}, \text{DIO}\}$  in the previous section.

### B. Framework of Assisted Coherence Distillation

In the task of assisted coherence distillation, Alice and Bob work together to transform a given quantum state  $\rho_{AB}$  (not necessarily pure) to an MCS in the system  $B$  such that the error is within certain threshold and the obtained MCS has dimension as large as possible, under the constraint that the available quantum operations are chosen from  $\mathcal{F}$ . We call this task the assisted coherence distillation since we can think of Alice as a helpful environment which holds an *extension*  $\rho_{AB}$  of  $\rho_B$  possessing a certain amount of quantum coherence. See Figure 2 for illustration. More formally, for any free operation class  $\mathcal{F}$ , any given state  $\rho_{AB} \in \mathcal{S}(AB)$  and error tolerance  $\varepsilon \in [0, 1]$ , the *one-shot assisted distillable coherence* of  $\rho_{AB}$  is defined as

$$C_{d,\mathcal{F}}^\varepsilon(\rho_{AB}) := \max \left\{ \log |B'| : \right. \\ \left. P(\text{Tr}_{A'} \Lambda(\rho_{AB}), \Psi_{B'}) \leq \varepsilon, \Lambda_{AB \rightarrow A'B'} \in \mathcal{F} \right\}, \quad (31)$$

where system  $A'$  is at Alice's hand, system  $B'$  is at Bob's hand, and  $|\Psi_{B'}\rangle$  is an MCS in  $B'$ .

### C. Framework of Assisted Incoherent Randomness Extraction

The task of assisted incoherent randomness extraction aims to obtain as many random bits as possible at Bob's laboratory that is secure from possible attackers such as Eve, under the assistance of a helpful friend Alice. In the beginning, Alice and Bob share a bipartite quantum state  $\rho_{AB}$  with purification  $|\psi\rangle_{RAB}$  such that the reference system  $R$  held by Eve. A general assisted incoherent randomness extraction protocol is characterized by a triplet  $(\Lambda, \Delta, f)$ , where  $\Lambda \in \mathcal{F}$ , and is composed of three steps:

- 1) Alice and Bob perform a free operation  $\Lambda_{AB \rightarrow A'B'} \in \mathcal{F}$  on their joint system. Let  $U_{AB \rightarrow A'B'E}$  be a Stinespring

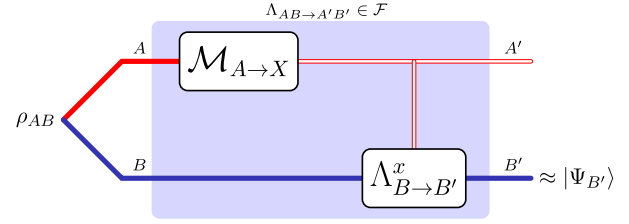


Fig. 2. Schematic diagram of the assisted coherence distillation. Alice and Bob together perform a free bipartite quantum operation  $\Lambda_{AB \rightarrow A'B'} \in \mathcal{F}$  to distill an MCS  $|\Psi_{B'}\rangle$ . The systems in red belong to Alice and the systems in blue belong to Bob. The shaded box depicts a one-way LQICC strategy in which Alice performs a measurement  $\mathcal{M}_{A \rightarrow X}$  and sends the outcome  $x$  to Bob. Conditioned on  $x$ , Bob performs an incoherent operation  $\Lambda_{B \rightarrow B'}^x$  to distill  $|\Psi_{B'}\rangle$ .

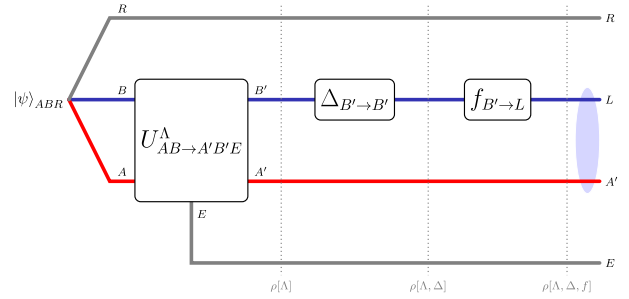


Fig. 3. Schematic diagram of an assisted incoherent randomness extraction protocol given by  $[\Lambda, \Delta, f]$ . The systems in red belong to Alice, the systems in blue belong to Bob, and the systems in gray belong to Eve.

isometry representation of  $\Lambda$ . We assume the environment system  $E$  of  $\Lambda$  is also controlled by Eve. Since Alice is a friend of Bob, Eve has no access to system  $A'$ . Hence Eve has control over two systems  $ER$ . After the action of  $\Lambda$ , the whole system is in a pure state

$$\rho[\Lambda]_{A'B'ER} := U_{AB \rightarrow A'B'E}(|\psi\rangle\langle\psi|_{RAB})U_{AB \rightarrow A'B'E}^\dagger. \quad (32)$$

- 2) Bob dephases system  $B'$  via the dephasing channel  $\Delta_{B'}$ . This yields the classical-quantum state

$$\rho[\Lambda, \Delta]_{A'B'ER} := \Delta_{B'}(\rho[\Lambda]_{A'B'ER}) \\ = \sum_{b \in \mathcal{B}} p_b |b\rangle\langle b|_{B'} \otimes \sigma_{A'ER}^b, \quad (34)$$

where  $p_b := \text{Tr}\langle b|\rho[\Lambda]_{A'B'ER}|b\rangle$  and  $\sigma_{A'ER}^b := \langle b|\rho[\Lambda]_{A'B'ER}|b\rangle/p_b$ .

- 3) A hash function  $f$  is applied on  $B'$  to extract the randomness that is *secure from Eve*, leading to the final output state

$$\rho[\Lambda, \Delta, f]_{A'LER} := \rho[\Lambda, \Delta]_{A'f(B')ER} \\ = \sum_{b \in \mathcal{B}} p_b |f(b)\rangle\langle f(b)|_L \otimes \sigma_{A'ER}^b. \quad (35)$$

A detailed procedure of the assisted randomness extraction via  $(\Lambda, \Delta, f)$  is depicted in Figure 3.

Using the security measure (9), the *one-shot assisted extractable randomness* of  $\rho_{AB}$  via  $\Lambda$  is defined as

$$\ell_\Lambda^\varepsilon(\rho_{AB}) := \max_f \{ \log |L| : d_{\text{sec}}(\rho[\Lambda, \Delta, f]_{LER}|ER) \leq \varepsilon \}. \quad (37)$$



Correspondingly, the *one-shot assisted extractable randomness* of  $\rho_{AB}$  is defined as

$$\ell_{\mathcal{F}}^{\varepsilon}(\rho_{AB}) := \max_{\Lambda \in \mathcal{F}} \ell_{\Lambda}^{\varepsilon}(\rho_{AB}). \quad (38)$$

Notice that the identity map  $\text{id}_{AB \rightarrow AB}$  is free in this distributed framework, thus  $(\text{id}_{AB \rightarrow AB}, \Delta_B, f)$  is an valid assisted incoherent randomness extraction protocol for any hash function  $f$ . In this protocol, Bob does not perform any assisted incoherent operation and directly dephases his state  $\psi_B \equiv \text{Tr}_{RA} \psi_{RAB}$  via  $\Delta_B$ . Hence, the environment system  $\mathcal{H}_E$  ceases to exist and we concern with the extractable randomness in state  $\Delta_B(\psi_{RB})$  that is secure from  $R$ . Following the argument around (12), we conclude for any  $\eta \in (0, \varepsilon]$  that

$$\ell_{\mathcal{F}}^{\varepsilon}(\rho_{AB}) \geq H_{\min}^{\varepsilon-\eta}(B|R)_{\sigma} + 4 \log \eta - 3, \quad (39)$$

where  $\sigma_{RAB} := \Delta_B(\psi_{RAB})$  is the dephased classical-quantum state and  $H_{\min}^{\varepsilon}$  is defined in (13).

*Remark 11:* In the above assisted randomness extraction framework, we do not require that the extracted randomness by Bob is secure from Alice. That is,  $L$  and  $A'$  may be classically correlated in the output state  $\rho[\Lambda, \Delta, f]_{A'LER}$  (cf. the shaded area of Figure 3). This assumption is reasonable since we regard Alice as a benevolent friend of Bob who aims to extract randomness. We only require that the extracted randomness be secure from the evil Eve who controls the systems  $ER$ .

*Remark 12:* Assume that Bob ignores the assistance from Alice, i.e., Bob performs a free operation  $\Lambda_{B \rightarrow B'} \in \text{DIO}$  (which is also free in the assisted framework) to extract randomness without touching  $A$ , we recover a slightly more general randomness extraction framework than that was investigated in Section III-C by allowing the state shared between  $B$  and the reference system  $R$  to be a mixed state  $\psi_{RB} = \text{Tr}_A \psi_{RAB}$ . Whereas in Section III-C,  $\psi_{RB}$  is assumed to be pure *a priori*.

*Remark 13:* Recently, Yang, Horodecki and Winter initiated the research of distributed private randomness distillation [68], in which Alice and Bob trust each other and collaborate to extract independent randomness private against Eve. Our assisted randomness extraction task is different from theirs mainly in two aspects: First, we do not require that Alice and Bob share independent randomness. All we need is that Bob possesses randomness private against Eve. Second, our free operations are naturally motivated within the resource theory of quantum coherence towards the distributed scenario, which is different from their closed local operations and dephasing channel communication. They mentioned in the Outlook section that the distributed randomness extraction under the framework of coherence theory is a notable topic to pursue. Our assisted randomness extraction task investigated here is the first step towards this direction.

#### D. Relation Between Assisted Coherence Distillation and Assisted Incoherent Randomness Extraction

We present an equivalent relation between the assisted coherence distillation and the assisted incoherent randomness extraction in the one-shot regime, extending Proposition 1 to the assisted scenario.

*Theorem 3 (Exact One-Shot Connection):* Let  $\rho_{AB}$  be a bipartite quantum state and  $\varepsilon \in [0, 1]$ . It holds that

$$C_{d, \text{QIP}}^{\varepsilon}(\rho_{AB}) = \ell_{\text{QIP}}^{\varepsilon}(\rho_{AB}). \quad (40)$$

The proof of Theorem 3 is divided into two pieces: we first conclude the “ $\leq$ ” direction in Lemma 1 and then prove the “ $\geq$ ” direction in Lemma 2. Actually, for the “ $\leq$ ” direction, we can obtain a much stronger statement that  $C_{d, \mathcal{F}}^{\varepsilon}(\rho_{AB}) \leq \ell_{\mathcal{F}}^{\varepsilon}(\rho_{AB})$  for arbitrary  $\mathcal{F}$ . That is, the optimal rate of assisted randomness extraction is always larger than the optimal rate of assisted coherence distillation.

*Lemma 1:* Let  $\mathcal{F} \in \{\text{LICC}, \text{LQICC}, \text{SI}, \text{SQI}, \text{QIP}\}$ . Let  $\rho_{AB}$  be a bipartite quantum state and  $\varepsilon \in [0, 1]$ . It holds that

$$C_{d, \mathcal{F}}^{\varepsilon}(\rho_{AB}) \leq \ell_{\mathcal{F}}^{\varepsilon}(\rho_{AB}). \quad (41)$$

*Proof:* This is shown by the same technique employed in proving Theorem 1. Nevertheless, we write down the details for completeness. Let  $C_{d, \mathcal{F}}^{\varepsilon}(\rho_{AB}) = \log M$  and let  $\Lambda_{AB \rightarrow A'B'} \in \mathcal{F}$  achieves this rate, i.e.,  $P(\text{Tr}_{A'} \Lambda_{AB \rightarrow A'B'}(\rho_{AB}), \Psi_{B'}) \leq \varepsilon$  and  $|B'| = M$ . Consider the following assisted randomness extraction protocol  $(\Lambda, \Delta, \text{id})$ , where the hash function is chosen as the identity map  $\text{id}$ . Since  $\rho[\Lambda]_{A'B'ER}$  purifies  $\Lambda_{AB \rightarrow A'B'}(\rho_{AB})$  (it also purifies  $\text{Tr}_{A'} \Lambda_{AB \rightarrow A'B'}(\rho_{AB})$ ) and  $\Psi_{B'}$  is a pure state, the Uhlmann’s theorem [66] guarantees that there exists a quantum state  $\sigma_{A'ER}^*$  in  $A'ER$  such that

$$\begin{aligned} & P(\text{Tr}_{A'} \Lambda_{AB \rightarrow A'B'}(\rho_{AB}), \Psi_{B'}) \\ &= P(\rho[\Lambda]_{A'B'ER}, \Psi_{B'} \otimes \sigma_{A'ER}^*). \end{aligned} \quad (42)$$

Consider the following chain of inequalities regarding state  $\rho[\Lambda]_{LER}$ :

$$\begin{aligned} & d_{\text{sec}}(\rho[\Lambda, \Delta, \text{id}]_{LER}|ER) \\ &:= \min_{\sigma_{ER} \in \mathcal{S}(ER)} P(\rho[\Lambda, \Delta, \text{id}]_{LER}, \pi_L \otimes \sigma_{ER}) \end{aligned} \quad (43)$$

$$\stackrel{(a)}{\leq} P(\rho[\Lambda, \Delta, \text{id}]_{LER}, \pi_L \otimes \sigma_{ER}^*) \quad (44)$$

$$\stackrel{(b)}{=} P((\Delta_{B'} \otimes \text{Tr}_{A'}) (\rho[\Lambda]_{A'B'ER}), (\Delta_{B'} \otimes \text{Tr}_{A'}) (\Psi_{B'} \otimes \sigma_{A'ER}^*)) \quad (45)$$

$$\stackrel{(c)}{\leq} P(\rho[\Lambda]_{A'B'ER}, \Psi_{B'} \otimes \sigma_{A'ER}^*) \quad (46)$$

$$\stackrel{(d)}{=} P(\text{Tr}_{A'} \Lambda_{AB \rightarrow A'B'}(\rho_{AB}), \Psi_{B'}) \quad (47)$$

$$\leq \varepsilon, \quad (48)$$

where  $\sigma_{ER}^* := \text{Tr}_{A'} \sigma_{A'ER}$  in (a), (b) follows from  $L \equiv B'$  and  $\Delta_{B'}(\Psi_{B'}) = \pi_{B'}$ , (c) follows from the data-processing of purified distance, and (d) follows from (42). That is,  $\log M$  is an achievable assisted randomness extraction rate, yielding the desired inequality. ■

The “ $\geq$ ” direction in (40) turns out to be more difficult. We first present a technical result that is utilized in the proof of this direction. This result is of independent interest as it offers a systematic method to construct an assisted coherence distillation protocol from a given assisted randomness extraction protocol (that does not use free operations) with the same performance.

*Proposition 3:* Let  $\text{id}_{AB \rightarrow AB}$  is the identity map. Given an assisted randomness extraction protocol  $(\text{id}, \Delta, f)$  such that  $d_{\text{sec}}(\rho[\text{id}, \Delta, f]_{LR}|R) \leq \varepsilon$ , we can construct from the protocol a quantum operation  $\Gamma : AB \rightarrow L$  such that  $\Gamma \in \text{QIP}$  and  $P(\Gamma_{AB \rightarrow L}(\rho_{AB}), \Psi_L) \leq \varepsilon$ , where  $L$  is in Bob's possession.

The proof is given at the end of this section.

*Remark 14:* We emphasize that this technical result holds for the QIP class, i.e., we can only show that the devised quantum operation  $\Gamma$  belongs to QIP. This limits us to enhance Theorem 3 (more concretely Lemma 2 below) to other free classes of operations. It remains an interesting problem whether one can further construct a distillation operation  $\Gamma$  that belongs to a less powerful free class such as LICC. As a possible solution, we conceive an alternative definition of the assisted incoherent randomness extraction task in Appendix B. For this new variant, we can establish the equivalence relation (40) for all free operation classes under consideration. However, we have difficulty in obtaining one-shot achievability bound for that new task; the lower bound concluded in (39) does not hold anymore. We left it as an open problem to obtain complete characterization (one-shot, second order, and asymptotic analyses) for that task.

*Lemma 2:* Let  $\rho_{AB}$  be a bipartite quantum state and  $\varepsilon \in [0, 1]$ . It holds that

$$C_{a, \text{QIP}}^{\varepsilon}(\rho_{AB}) \geq \ell_{\text{QIP}}^{\varepsilon}(\rho_{AB}). \quad (49)$$

*Proof:* Let  $\ell_{\text{QIP}}^{\varepsilon}(\rho_{AB}) = \log |L|$  and let the randomness extraction protocol  $(\Lambda, \Delta, f)$  with  $\Lambda_{AB \rightarrow A'B'} \in \text{QIP}$  achieves this rate, i.e.,  $d_{\text{sec}}(\rho[\Lambda, \Delta, f]_{LER}|ER) \leq \varepsilon$ . The key observation is that applying the randomness extraction protocol  $(\Lambda, \Delta, f)$  on quantum state  $\rho_{AB}$  is the same as applying the randomness extraction protocol  $(\text{id}, \Delta, f)$  on quantum state  $\sigma_{A'B'} \equiv \Lambda_{AB \rightarrow A'B'}(\rho_{AB})$  with purification  $\rho[\Lambda]_{A'B'ER}$  and reference systems  $ER$ . For the latter protocol, Proposition 3 guarantees that there exists a quantum operation  $\Gamma_{A'B' \rightarrow L}$  such that  $\Gamma \in \text{QIP}$  and  $P(\Gamma(\sigma_{A'B'}), \Psi_L) \leq \varepsilon$ . Compositing these two quantum operations  $\Lambda$  and  $\Gamma$  yields

$$\begin{aligned} & P(\Gamma_{A'B' \rightarrow L} \circ \Lambda_{AB \rightarrow A'B'}(\rho_{AB}), \Psi_L) \\ &= P(\Gamma_{A'B' \rightarrow L}(\sigma_{A'B'}), \Psi_L) \leq \varepsilon. \end{aligned} \quad (50)$$

That is to say, the composite operation  $\Gamma \circ \Lambda$  distills an MCS of rank  $|L|$  such that the error is bounded by  $\varepsilon$ . Since  $\Lambda \in \text{QIP}$ ,  $\Gamma \in \text{QIP}$ , and the class QIP is closed under composition [67], we have  $\Gamma \circ \Lambda \in \text{QIP}$ . As so, we have constructed an operation in QIP that distills MCS at rate  $\log |L|$  and thus complete the proof. ■

Now we proceed to prove the claim in Proposition 3. The following lemma is utilized, whose proof can be checked by definition.

*Lemma 3:* Let  $|u_i\rangle$  and  $|v_i\rangle$  be the purification of  $\rho_i$  and  $\sigma_i$  such that  $F(\rho_i, \sigma_i) = \langle u_i | v_i \rangle$ . Then we have

$$\begin{aligned} & F\left(\sum_i p_i |i\rangle\langle i| \otimes \rho_i, \sum_i q_i |i\rangle\langle i| \otimes \sigma_i\right) \\ &= \sum_i \sqrt{p_i q_i} F(\rho_i, \sigma_i) \\ &= F\left(\sum_i \sqrt{p_i} |i\rangle |u_i\rangle, \sum_i \sqrt{q_i} |i\rangle |v_i\rangle\right). \end{aligned} \quad (51)$$

*Proof of Proposition 3:* Let  $\sigma_R^*$  be a quantum state that attains the minimum in

$$\begin{aligned} & d_{\text{sec}}(\rho[\text{id}, \Delta, f]_{LR}|R) \\ &:= \min_{\sigma_R \in \mathcal{S}(R)} P(\rho[\text{id}, \Delta, f]_{LR}, \pi_L \otimes \sigma_R). \end{aligned} \quad (52)$$

and then we have

$$P(\rho[\text{id}, \Delta, f]_{LR}, \pi_L \otimes \sigma_R^*) \leq \varepsilon \quad (53)$$

The relation between purified distance  $P$  and fidelity  $F$  gives

$$F(\rho[\text{id}, \Delta, f]_{LR}, \pi_L \otimes \sigma_R^*) \geq \sqrt{1 - \varepsilon^2}. \quad (54)$$

We decompose the pure tripartite state  $|\psi\rangle_{RAB}$  into the basis  $\mathcal{B}$  of system  $B$  as

$$|\psi\rangle_{RAB} := \sum_{b \in \mathcal{B}} \sqrt{p_B(b)} |b\rangle_B |\psi^b\rangle_{RA}, \quad (55)$$

where  $p_B$  a probability distribution and  $\{|\psi^b\rangle\}$  a set of pure states in  $RA$  which are not necessarily mutually orthogonal. Define the incoherent isometry  $U_f$  from  $\mathcal{H}_B$  to  $\mathcal{H}_{LB}$  such that

$$\forall b \in \mathcal{B}, U_f |b\rangle_B := |f(b)\rangle_L |b\rangle_B. \quad (56)$$

Notice that

$$U_f |\psi\rangle_{ABR} = \sum_{b \in \mathcal{B}} \sqrt{p_B(b)} U_f |b\rangle_B |\psi^b\rangle_{RA} \quad (57)$$

$$= \sum_{b \in \mathcal{B}} \sqrt{p_B(b)} |f(b)\rangle_L |b\rangle_B |\psi^b\rangle_{RA}. \quad (58)$$

Since the mapping  $f : \mathcal{B} \rightarrow \mathcal{L}$  is non-injective, where  $\mathcal{L}$  is the alphabet of  $L$ , each new basis  $\ell$  may corresponds to several bases  $b$  such that  $f(b) = \ell$ . As so, we can equivalently write  $U_f |\psi\rangle_{ABR}$  as

$$U_f |\psi\rangle_{ABR} = \sum_{\ell \in \mathcal{L}} \sqrt{r_\ell} |\ell\rangle_L \otimes |\phi^\ell\rangle_{RAB}, \quad (59)$$

where the normalized vectors  $|\phi^\ell\rangle_{RAB}$  and normalization factors  $r_\ell$  for  $\ell \in \mathcal{L}$  satisfy

$$\sqrt{r_\ell} |\phi^\ell\rangle_{RAB} := \sum_{b \in \mathcal{B}: f(b)=\ell} \sqrt{p_B(b)} |b\rangle_B \otimes |\psi^b\rangle_{RA}. \quad (60)$$

Let  $|\phi^*\rangle_{RAB}$  on  $\mathcal{H}_{RAB}$  be a purification of  $\sigma_R^*$ . By the Uhlmann's theorem [66], for each  $|\phi^\ell\rangle_{RAB}$  there exists a unitary  $U_\ell$  on  $\mathcal{H}_{AB}$  such that

$$F(\text{Tr}_{AB} |\phi^\ell\rangle\langle\phi^\ell|_{RAB}, \sigma_R^*) = F(U_\ell |\phi^\ell\rangle_{RAB}, |\phi^*\rangle_{RAB}). \quad (61)$$

Define the conditional unitary  $U := \sum_{\ell \in \mathcal{L}} |\ell\rangle\langle\ell|_L \otimes U_\ell$ . We have

$$\begin{aligned} & F(U U_f |\psi\rangle_{RAB}, |\Psi\rangle_L \otimes |\phi^*\rangle_{RAB}) \\ &\stackrel{(a)}{=} F\left(\sum_{\ell \in \mathcal{L}} \sqrt{r_\ell} |\ell\rangle_L \otimes U_\ell |\phi^\ell\rangle_{RAB}, \sum_{\ell \in \mathcal{L}} \frac{1}{\sqrt{|\mathcal{L}|}} |\ell\rangle_L \otimes |\phi^*\rangle_{RAB}\right) \end{aligned} \quad (62)$$

$$\stackrel{(b)}{=} \sum_{\ell \in \mathcal{L}} \sqrt{\frac{r_\ell}{|\mathcal{L}|}} F(U_\ell |\phi^\ell\rangle_{RAB}, |\phi^*\rangle_{RAB}) \quad (63)$$

$$\stackrel{(c)}{=} \sum_{\ell \in \mathcal{L}} \sqrt{\frac{r_\ell}{|\mathcal{L}|}} F(\text{Tr}_{AB} |\phi_\ell\rangle\langle\phi_\ell|_{RAB}, \sigma_R^*) \quad (64)$$

$$\stackrel{(d)}{=} F \left( \sum_{\ell \in \mathcal{L}} r_\ell |\ell\rangle\langle\ell|_L \otimes \text{Tr}_{AB} |\phi_\ell\rangle\langle\phi_\ell|_{RAB}, \sum_{\ell \in \mathcal{L}} \frac{1}{|\mathcal{L}|} |\ell\rangle\langle\ell|_L \otimes \sigma_R^* \right) \quad (65)$$

$$\stackrel{(e)}{=} F(\rho[\text{id}, \Delta, f]_{LR}, \pi_L \otimes \sigma_R^*), \quad (66)$$

where (a) follows by definition, (b) and (d) follow from Lemma 3, (c) follows from Eq. (61), and (e) follows from the fact that

$$\rho[\text{id}, \Delta, f]_{LR} = \text{Tr}_{AB} U_f \Delta_B (\Psi_{RAB}) U_f^\dagger \quad (67)$$

$$= \sum_{\ell \in \mathcal{L}} r_\ell |\ell\rangle\langle\ell|_L \otimes \text{Tr}_{AB} |\phi_\ell\rangle\langle\phi_\ell|_{RAB}. \quad (68)$$

Now we construct the required operation  $\Gamma_{AB \rightarrow L}$  as

$$\Gamma_{AB \rightarrow L}(\cdot) := \text{Tr}_{AB} [U U_f (\cdot) U_f^\dagger U^\dagger]. \quad (69)$$

See Figure 4 for illustration of this construction. First we show that  $\Gamma_{AB \rightarrow L}$  can transform  $\rho_{AB}$  to an MCS  $\Psi_L$  within error  $\varepsilon$ . Consider the following chain of inequalities:

$$F(\Gamma_{AB \rightarrow L}(\rho_{AB}), |\Psi\rangle\langle\Psi|_L) = F(\text{Tr}_{AB} [U U_f \rho_{AB} U_f^\dagger U^\dagger], |\Phi\rangle\langle\Phi|_L) \quad (70)$$

$$\stackrel{(a)}{\geq} F(U U_f |\psi\rangle_{RAB}, |\Phi\rangle_L \otimes |\phi^*\rangle_{RAB}) \quad (71)$$

$$\stackrel{(b)}{\stackrel{=}{\geq}} F(\rho[\text{id}, \Delta, f]_{LR}, \pi_L \otimes \sigma_R^*) \quad (72)$$

$$\stackrel{(c)}{\geq} \sqrt{1 - \varepsilon^2}, \quad (73)$$

where (a) follows by the data-processing inequality of the fidelity  $F$  under  $\text{Tr}_{AB}$ , (b) follows by (66), and (c) follows from (54). This implies that  $P(\Gamma_{AB \rightarrow L}(\rho_{AB}), \Psi_L) \leq \varepsilon$ . It remains to check that  $\Gamma_{AB \rightarrow L} \in \text{QIP}$ . Note that  $\Gamma$  admits the following Kraus decomposition

$$\Gamma(\cdot) = \sum_{b \in \mathcal{B}} K_b U_f (\cdot) U_f^\dagger K_b^\dagger \quad (74)$$

with operators  $K_b := \langle b|U$ . This is indeed a Kraus decomposition since

$$\begin{aligned} \sum_{b \in \mathcal{B}} (U_f^\dagger K_b^\dagger) (K_b U_f) &= U_f^\dagger \left( \sum_{b \in \mathcal{B}} K_b^\dagger K_b \right) U_f \\ &= U_f^\dagger U^\dagger \left( \sum_{b \in \mathcal{B}} |b\rangle\langle b|_B \right) U U_f = U_f^\dagger U^\dagger U U_f = \mathbf{1}. \end{aligned} \quad (75)$$

On the other hand, one can verify that for any bases  $b, b' \in \mathcal{B}$  and any quantum state  $\rho_A^{b'}$  in  $A$ ,

$$K_b U_f (|b'\rangle\langle b'|_B \otimes \rho_A^{b'}) U_f^\dagger K_b^\dagger = \text{Tr} [K_b \rho_A^{b'} K_b^\dagger] | \langle b|U_f(b')|b'\rangle|^2 |f(b')\rangle\langle f(b')|_L \quad (76)$$

$$\in \mathcal{I}^{**}(L). \quad (77)$$

That is to say,  $\Gamma$  transforms arbitrary quantum-incoherent state in  $\mathcal{QI}$  to some incoherent state in  $\mathcal{I}$ , which in turn is a strict

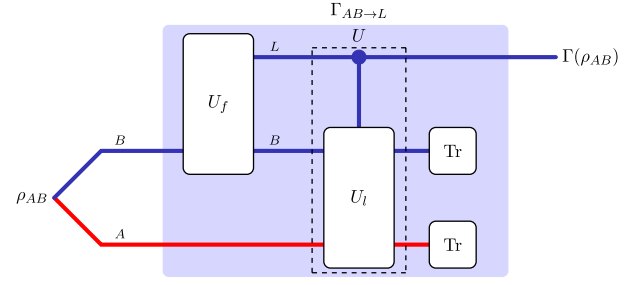


Fig. 4. Schematic diagram of the QIP distillation protocol in Proposition 3. The systems in red belong to Alice and the systems in blue belong to Bob. The isometry  $U_f$  and conditional unitary  $U$  in the dashed box are not necessarily incoherent. The shaded area depicts the designed operation  $\Gamma_{AB \rightarrow L}$ , which belongs to QIP.

subset of  $\mathcal{QI}$ . Thus we conclude that  $\Gamma \in \text{QIP}$  and complete the proof.  $\blacksquare$

### E. Second Order Analysis

We now give second order characterizations to both assisted coherence distillation and assisted randomness extraction. We do so by first establishing one-shot achievability and converse bounds for these two tasks in terms of the hypothesis testing relative entropy. These two bounds have matching dependence on the error threshold  $\varepsilon$ . Then we derive a second order characterization by invoking the second order expansion of the hypothesis testing relative entropy. As a direct corollary, we show that the ultimate rate in the asymptotic setting is uniquely determined by the quantum incoherent relative entropy of coherence.

**Theorem 4 (One-Shot Characterization):** Let the operation class  $\mathcal{F} \in \{\text{LICC}, \text{LQICC}, \text{SI}, \text{SQI}, \text{QIP}\}$ . Let  $\rho_{AB}$  be a bipartite quantum state and  $\varepsilon \in (0, 1)$ . For arbitrary  $\eta \in (0, \varepsilon)$  and  $\delta \in (0, \min\{(\varepsilon - \eta)^2/3, 1 - (\varepsilon - \eta)^2\})$ , it holds that

$$D_H^{(\varepsilon - \eta)^2 - 2\delta}(\rho_{AB} \| \Delta_B(\rho_{AB})) - c(\rho_{AB}, \varepsilon, \delta, \eta) \stackrel{(a)}{\leq} \ell_{\mathcal{F}}^\varepsilon(\rho_{AB}) \quad (78a)$$

$$\stackrel{(b)}{\leq} \ell_{\text{QIP}}^\varepsilon(\rho_{AB}) \quad (78b)$$

$$\stackrel{(c)}{=} C_{d, \text{QIP}}^\varepsilon(\rho_{AB}) \quad (78c)$$

$$\stackrel{(d)}{\leq} D_H^{\varepsilon^2}(\rho_{AB} \| \Delta_B(\rho_{AB})), \quad (78d)$$

where the correction term  $c$  is defined as

$$\begin{aligned} c(\rho_{AB}, \varepsilon, \delta, \eta) &:= \log \theta(\rho_{AB}) + \log \theta(\Delta_B(\rho_{AB})) \\ &\quad + \log((\varepsilon - \eta)^2 - \delta) + 11 \\ &\quad - \log(\delta^5 \eta^4 (\varepsilon - \eta)^2 (1 - (\varepsilon - \eta)^2 + \delta)). \end{aligned} \quad (79)$$

The proof of Theorem 4 is divided into the following steps: the achievability part (a) is drawn in Lemma 4; the inequality (b) follows directly from the inclusion relation (30); the equality (c) has already been shown in Theorem 3; and the converse part (d) is proved in Lemma 5. However, we note that the one-shot characterization for the assisted coherence distillation  $C_{d, \text{QIP}}^\varepsilon(\rho_{AB})$  cannot be generalized to other classes of free operations since (c) only holds for QIP.

**Lemma 4 (Achievability):** Let the operation class  $\mathcal{F} \in \{\text{LICC}, \text{LQICC}, \text{SI}, \text{SQI}, \text{QIP}\}$ . Let  $\rho_{AB}$  be a bipartite

quantum state and  $\varepsilon \in (0, 1)$ . For arbitrary  $\eta \in (0, \varepsilon)$  and  $\delta \in (0, \min\{(\varepsilon - \eta)^2/3, 1 - (\varepsilon - \eta)^2\})$ , it holds that

$$\ell_{\mathcal{F}}^{\varepsilon}(\rho_{AB}) \geq D_H^{(\varepsilon-\eta)^2-2\delta}(\rho_{AB} \|\Delta_B(\rho_{AB})) - c(\rho_{AB}, \varepsilon, \delta, \eta). \quad (80)$$

where the correction term  $c$  is defined in (79).

*Proof:* In (39) we already obtained the following lower bound for arbitrary free class  $\mathcal{F}$  in terms of the smooth conditional min-entropy:

$$\ell_{\mathcal{F}}^{\varepsilon}(\rho_{AB}) \geq H_{\min}^{\varepsilon-\eta}(B|R)_{\sigma} + 4 \log \eta - 3, \quad (81)$$

where  $\sigma_{RAB} := \Delta_B(|\psi\rangle\langle\psi|_{RAB})$  is the dephased classical-quantum state. Moreover, we establish in Proposition 4 a relation between the smooth min entropy  $H_{\min}^{\varepsilon}$  and the hypothesis testing relative entropy  $D_H^{\varepsilon}$  regarding state  $\sigma_{RAB}$ . Adapting (101) into (81), we have the desired (80). ■

Our converse bound proved below asserts that the quantum-incoherent hypothesis testing relative entropy of coherence upper bounds the one-shot assisted distillable coherence of  $\rho_{AB}$  via arbitrary free operations  $\mathcal{F} \in \{\text{LICC}, \text{LQICC}, \text{SI}, \text{SQI}, \text{QIP}\}$ . This result can be viewed as a one-shot analog of [43, Theorem 2], in which Streltsov *et al.* showed that the quantum-incoherent relative entropy of coherence upper bounds the asymptotic assisted distillable coherence of  $\rho_{AB}$ . Note that  $(d)$  in (78d) is immediately concluded from Lemma 5 by choosing  $\sigma_{AB} \equiv \Delta_B(\rho_{AB})$  in (82).

*Lemma 5 (Converse):* Let the operation class  $\mathcal{F} \in \{\text{LICC}, \text{LQICC}, \text{SI}, \text{SQI}, \text{QIP}\}$ . Let  $\rho_{AB}$  be a bipartite quantum state and  $\varepsilon \in (0, 1)$ . It holds that

$$C_{d,\mathcal{F}}^{\varepsilon}(\rho_{AB}) \leq \min_{\sigma_{AB} \in \mathcal{QI}} D_H^{\varepsilon^2}(\rho_{AB} \|\sigma_{AB}). \quad (82)$$

*Proof:* Assume  $C_{d,\mathcal{F}}^{\varepsilon}(\rho_{AB}) = \log M$ , that is, there exists a free operation  $\mathcal{D}_{AB \rightarrow C} \in \mathcal{F}$  such that

$$P(\mathcal{D}_{AB \rightarrow C}(\rho_{AB}), \Psi_M) \leq \varepsilon. \quad (83)$$

By the definition of purified distance  $P$ , the above condition is equivalent to

$$\text{Tr}[\mathcal{D}_{AB \rightarrow C}(\rho_{AB})\Psi_M] \geq 1 - \varepsilon^2. \quad (84)$$

Let  $M_{AB} := \mathcal{D}^{\dagger}(\Psi_M)$ , where  $\mathcal{D}^{\dagger}$  is the adjoint of  $\mathcal{D}$ . Since  $\mathcal{D}$  is completely positive, so is  $\mathcal{D}^{\dagger}$ . This gives  $M_{AB} \geq 0$ . On the other hand,  $\text{Tr}[\mathcal{D}_{AB \rightarrow C}(\rho_{AB})\Psi_M] \leq 1$  implies  $M_{AB} \leq \mathbb{1}_{AB}$ . Now we have

$$\text{Tr}[\rho_{AB}M_{AB}] = \text{Tr}[\rho_{AB}\mathcal{D}^{\dagger}(\Psi_M)] \quad (85)$$

$$= \text{Tr}[\mathcal{D}(\rho_{AB})\Psi_M] \geq 1 - \varepsilon^2. \quad (86)$$

That is to say,  $M_{AB}$  is a feasible solution for  $D_H^{\varepsilon^2}(\rho_{AB} \|\sigma_{AB})$ . Then

$$D_H^{\varepsilon^2}(\rho_{AB} \|\sigma_{AB}) \geq -\log \text{Tr}[\sigma_{AB}M_{AB}] \quad (87)$$

$$= -\log \text{Tr}[\sigma_{AB}\mathcal{D}^{\dagger}(\Psi_M)] \quad (88)$$

$$= -\log \text{Tr}[\mathcal{D}(\sigma_{AB})\Psi_M]. \quad (89)$$

Since  $\mathcal{D}$  is quantum-incoherent state preserving, we know that  $\mathcal{D}(\sigma_{AB})$  is an incoherent state in  $\mathcal{C}$  and thus  $\text{Tr}[\mathcal{D}(\sigma_{AB})\Psi_M] \leq 1/M$ . Then we have

$D_H^{\varepsilon^2}(\rho_{AB} \|\sigma_{AB}) \geq -\log 1/M = C_{d,\mathcal{F}}^{\varepsilon}(\rho_{AB})$ . As the argument holds for any  $\sigma \in \mathcal{QI}$ , we can complete the proof by minimize over  $\sigma$ . ■

The matching dependence on the error parameter  $\varepsilon$  of the achievable and converse bounds in Theorem 4 yields tight second order expansions of the assisted distillable coherence as well as the assisted incoherent extractable randomness.

*Theorem 5 (Second Order Expansion):* Let the operation class  $\mathcal{F} \in \{\text{LICC}, \text{LQICC}, \text{SI}, \text{SQI}, \text{QIP}\}$ . Let  $\rho_{AB}$  be a bipartite quantum state and  $\varepsilon \in [0, 1]$ . The following second order expansions hold:

$$C_{d,\text{QIP}}^{\varepsilon}(\rho_{AB}^{\otimes n}) = nD(\rho_{AB} \|\Delta_B(\rho_{AB})) + \sqrt{nV(\rho_{AB} \|\Delta_B(\rho_{AB}))}\Phi^{-1}(\varepsilon^2) + O(\log n), \quad (90)$$

$$\ell_{\mathcal{F}}^{\varepsilon}(\rho_{AB}^{\otimes n}) = nD(\rho_{AB} \|\Delta_B(\rho_{AB})) + \sqrt{nV(\rho_{AB} \|\Delta_B(\rho_{AB}))}\Phi^{-1}(\varepsilon^2) + O(\log n). \quad (91)$$

*Proof:* The proof follows from Theorem 4 and a similar argument of the proof of Theorem 2. ■

*Remark 15:* From Proposition 4 in Section VI, the first and second order asymptotics can also be written as conditional entropy  $H(B|R)_{\sigma_{ABR}}$  and conditional information variance  $V(B|R)_{\sigma_{ABR}}$  respectively, where  $\sigma_{ABR} = \rho[\text{id}, \Delta]$  is the dephased classical-quantum state from the assisted randomness extraction protocol.

*Remark 16:* As a consequence of Theorem 5, we find the quantum-incoherent relative entropy of coherence, defined as  $C_R^{A|B}(\rho_{AB}) := \min_{\sigma_{AB} \in \mathcal{QI}} D(\rho_{AB} \|\sigma_{AB}) = D(\rho_{AB} \|\Delta_B(\rho_{AB}))$  [15, Eq. (4)], quantifies the ultimate power of assistance in both the coherence distillation and incoherent randomness extraction tasks, in the sense that it is the best distillation and extraction rates that can be achieved using the largest free class QIP in the distributed scenario. This bestows the quantum-incoherent relative entropy of coherence a new operational meaning.

*Remark 17:* Our results—the single-shot result in Theorem 4, the second order result in Theorem 5, and its corollary in Remark 16—together paint an ‘almost’ complete picture for the assisted coherence distillation task. What’s more, they cover many known results as special cases:

- 1) When  $\rho_{AB} = \rho_A \otimes \rho_B$  is a product state, our results reduce to the unassisted coherence distillation [14], as QIP reduces to MIO in the single party setting. Theorem 5 matches the second order results for the coherence distillation without assistance in Theorem 2.
- 2) When  $\rho_{AB}$  is pure or maximally correlated, Remark 16 enhances the results of Theorem 5 and Proposition 6 in [43] by stating that the quantum-incoherent relative entropy of coherence  $C_R^{A|B}(\rho_{AB})$  is the ultimate rate that can be achieved in the assisted coherence distillation even if we make use of the largest free operation class QIP. Note that the same conclusion was previously obtained in [67, Proposition 19] for the pure state case.

## V. STRONG CONVERSE PROPERTY

The direct part of resource distillation states that for any rate below the optimal rate, there is a corresponding distillation protocol that accomplishes the task successfully. More precisely, if we denote the transformation error in the protocol for  $n$  uses of the underlying resource by  $\varepsilon$ , then for any rate below the optimal rate there exists a protocol, whose transformation error  $\varepsilon$  vanishes in the asymptotic limit  $n \rightarrow +\infty$ . Such rates are called achievable, and the optimal rate is defined as the supremum over all achievable rates. In contrast, the converse part states that for any distillation protocol with a rate above the optimal rate, the error does not vanish asymptotically. That is, it is bounded away from 0 in the asymptotic limit  $n \rightarrow +\infty$ . This is usually called weak converse. In principle, it leaves open the possibility of a trade-off between the error and the rate of a protocol. However, the strong converse property rules out such a possibility, stating that for any distillation protocol with a rate above the optimal rate, the corresponding transformation error  $\varepsilon$  incurred in the protocol converges to one. In other words, such protocols become worse with increasing block length  $n$  and eventually fail with certainty in the asymptotic limit. In this part, we showcase a standard argument how a second order result automatically implies the strong converse property.

As a concrete example, we consider the task of unassisted coherence distillation whose strong converse property has been pointed out by [28, Theorem 16]. Here we give an alternative proof. For simplicity, we denote  $C_r(\rho) := D(\rho||\Delta(\rho))$  and  $V_r(\rho) := V(\rho||\Delta(\rho))$ . For any achievable rate  $R_n$ , we have  $R_n \leq \frac{1}{n}C_{d,\mathcal{O}}^\varepsilon(\rho^{\otimes n})$ . By Theorem 2, we have

$$R_n \leq C_r(\rho) + \sqrt{\frac{V_r(\rho)}{n}} \Phi^{-1}(\varepsilon^2) + f(n), \quad (92)$$

with  $f(n) \in O(\log n/n)$ . Rearranging (92) and using monotonicity of  $\Phi$  yields

$$\varepsilon^2 \geq \Phi\left(\sqrt{\frac{n}{V_r(\rho)}}(R_n - C_r(\rho)) + g(n)\right), \quad (93)$$

with  $g(n) = -\sqrt{n}f(n)/\sqrt{V_r(\rho)}$ . Thus  $\lim_{n \rightarrow +\infty} g(n) = 0$ . Note that  $\lim_{x \rightarrow +\infty} \Phi(x) = 1$ . For any achievable rate  $R_n > C_r(\rho)$ , the argument in (93) diverges to  $+\infty$  and thus we have  $\varepsilon \rightarrow 1$  as  $n \rightarrow \infty$ . This implies the strong converse property of coherence distillation under  $\mathcal{O} \in \{\text{MIO, DIO, IO, DIO}\}$ . Similar argument works for the incoherent randomness extraction.

Moreover, following the same argument outlined above, we can conclude from Theorem 5 that both the assisted coherence distillation via QIP and the assisted incoherent randomness extraction via arbitrary free operation class  $\mathcal{F} \in \{\text{LICC, LQICC, SI, SQI, QIP}\}$  satisfy the strong converse property. This promises the unique role of  $C_R^{A|B}(\rho_{AB})$  in the two assisted tasks.

## VI. RELATIONS AMONG ENTROPIES OF A DEPHASED TRIPARTITE QUANTUM STATE

Let  $\rho_{AB}$  be a bipartite quantum state with purification  $|\psi\rangle_{RAB}$ , i.e.,  $\text{Tr}_R \psi_{RAB} = \rho_{AB}$ . Assume the following

decomposition into the basis  $\mathcal{B}$  of system  $B$ :

$$|\psi\rangle_{RAB} := \sum_{b \in \mathcal{B}} \sqrt{p_B(b)} |b\rangle_B |\psi^b\rangle_{RA}, \quad (94)$$

where  $p_B$  a probability distribution and  $\{|\psi^b\rangle\}$  a set of pure states in  $AR$  which are not necessarily mutually orthogonal. By definition, we have  $\rho_{AB} = \text{Tr}_R \psi_{RAB}$ . Dephasing  $B$  yields the classical-quantum state

$$\sigma_{RAB} := \Delta_B(\psi_{RAB}) = \sum_{a \in \mathcal{B}} p_a |a\rangle\langle a|_B \otimes |\psi^a\rangle\langle \psi^a|_{RA}. \quad (95)$$

Notice that  $\sigma_{AB} = \Delta_B(\rho_{AB})$ . In the following, we establish a list of relations among the various entropies evaluated on the dephased quantum state  $\sigma_{RAB}$ . These relations are essential to the above second order analysis. They are of independent interest and may find applications in other quantum information processing tasks.

Before presenting the relations, we first introduce some notations. For two Hermitian operators  $X$  and  $Y$ , we denote by  $\{X \geq Y\}$  the projector onto the space spanned by the eigenvectors of  $X - Y$  with non-negative eigenvalues. Let  $\rho \in \mathcal{S}(\mathcal{H})$ ,  $\sigma \in \mathcal{P}(\mathcal{H})$ , and  $\varepsilon \in [0, 1]$ . The *information spectrum relative entropy* of  $\rho$  w.r.t.  $\sigma$  is defined as [22, Definition 8]

$$D_s^\varepsilon(\rho||\sigma) := \sup \{x : \text{Tr} \rho \{ \rho \leq 2^x \sigma \} \leq \varepsilon\}. \quad (96)$$

The Nussbaum and Szkoła's distributions are used intensively in the analysis that follows. Assume the eigenvalue decompositions  $\rho = \sum_x r_x |v_x\rangle\langle v_x|$  and  $\sigma = \sum_y s_y |u_y\rangle\langle u_y|$ . Their Nussbaum and Szkoła's distributions [69] are defined as  $P_{\rho,\sigma}(x, y) := r_x | \langle v_x | u_y \rangle |^2$  and  $Q_{\rho,\sigma}(x, y) := s_y | \langle v_x | u_y \rangle |^2$ . These distributions satisfy the property that

$$D(P_{\rho,\sigma}||Q_{\rho,\sigma}) = D(\rho||\sigma) \quad \text{and} \quad V(P_{\rho,\sigma}||Q_{\rho,\sigma}) = V(\rho||\sigma). \quad (97)$$

**Proposition 4:** Let  $\varepsilon \in (0, 1)$  and  $\delta \in (0, \min\{\varepsilon^2/3, 1 - \varepsilon^2\})$ . We have the following relations regarding the dephased tripartite quantum state  $\sigma_{RAB}$  (95):

$$D_s^\varepsilon(P_{\sigma_{BR}, \mathbb{1}_B \otimes \sigma_R} || Q_{\sigma_{BR}, \mathbb{1}_B \otimes \sigma_R}) = -D_s^{1-\varepsilon}(P_{\rho_{AB}, \Delta_B(\rho_{AB})} || Q_{\rho_{AB}, \Delta_B(\rho_{AB})}), \quad (98)$$

$$D(\sigma_{BR} || \mathbb{1}_B \otimes \sigma_R) = -D(\rho_{AB} || \Delta_B(\rho_{AB})), \quad (99)$$

$$V(\sigma_{BR} || \mathbb{1}_B \otimes \sigma_R) = V(\rho_{AB} || \Delta_B(\rho_{AB})), \quad (100)$$

$$H_{\min}^\varepsilon(B|R)_\sigma \geq D_H^{\varepsilon^2 - 2\delta}(\rho_{AB} || \Delta_B(\rho_{AB})) - c(\rho_{AB}, \varepsilon, \delta), \quad (101)$$

where the correction term is defined as

$$c(\rho_{AB}, \varepsilon, \delta) := \log \theta(\rho_{AB}) + \log \theta(\Delta_B(\rho_{AB})) + \log(\varepsilon^2 - \delta) - \log(\delta^5 \varepsilon^2 (1 - \varepsilon^2 + \delta)) + 8. \quad (102)$$

*Proof of Eq. (98):* For reduced state  $\sigma_R$  assume the spectral decompositions  $\sigma_R = \sum_r q_r |v_r^r\rangle\langle v_r^r|$ . For the reduced states  $\{\psi_R^b\}_b$ , assume the spectral decompositions

$$\psi_R^b = \sum_r p_{R|B}(r|b) |v^{r|b}\rangle\langle v^{r|b}|_R, \quad (103)$$

where  $p_{R|B}$  is a conditional probability distribution, and  $\{|v^r|^b\rangle\}$  is an orthonormal basis of  $R$  for each  $b$ . Set  $p_{BR} := p_{R|B}p_B$ , we have the following spectral decompositions

$$\mathbb{1}_B \otimes \sigma_R = \sum_{b,r} q_r |b\rangle\langle b|_B \otimes |v^r\rangle\langle v^r|_R, \quad (104)$$

$$\sigma_{BR} = \sum_{b,r} p_{BR}(b,r) |b\rangle\langle b|_B \otimes |v^r|^b\rangle\langle v^r|^b|_R. \quad (105)$$

Notice that  $\sigma_R$  and  $\rho_{AB}$  are two marginal states of pure tripartite state  $\Psi_{ABR}$  and thus they have the same eigenvalues due to the Schmidt theorem. That is, we can denote the eigenvalue decomposition of  $\rho_{AB}$  as  $\rho_{AB} = \sum_r q_r |u^r\rangle\langle u^r|$ , where  $\{|u^r\rangle\}$  is an orthonormal basis of  $AB$ . What's more, since each conditional state  $|\psi^b\rangle_{RA}$  (95) is pure, the two marginal states  $\psi_R^b$  and  $\psi_A^b$  has the same eigenvalues from the Schmidt theorem. That is, there exists  $\{|u^a|^b\rangle\}$  is an orthonormal basis of  $A$  for each  $b$  such that

$$|\psi^b\rangle_{RA} = \sum_r \sqrt{p_{R|B}(r|b)} |u^r|^b\rangle_A |v^r|^b\rangle_R. \quad (106)$$

Correspondingly, we can decompose  $\sigma_{AB}$  as

$$\sigma_{AB} = \Delta_B(\rho_{AB}) = \sum_{b,a} p_{BR}(b,a) |b\rangle\langle b|_B \otimes |u^a|^b\rangle\langle u^a|^b|_A, \quad (107)$$

Consider the Nussbaum and Szkoła's distributions for the operators  $\sigma_{BR}$  and  $\mathbb{1}_B \otimes \sigma_R$ :

$$\begin{aligned} P_{\sigma_{BR}, \mathbb{1}_B \otimes \sigma_R}((b', r'), (b, r)) \\ := P_{BR}(b, r') |\langle v_{r'}^b | v_r \rangle|^2 \delta_{bb'} = P_{BR}(b, r') |\langle v_{r'}^b | v_r \rangle|^2, \end{aligned} \quad (108a)$$

and

$$\begin{aligned} Q_{\sigma_{BR}, \mathbb{1}_B \otimes \sigma_R}((b', r'), (b, r)) \\ := q_r |\langle v_{r'}^b | v_r \rangle|^2 \delta_{bb'} = q_r |\langle v_{r'}^b | v_r \rangle|^2, \end{aligned} \quad (108b)$$

and the Nussbaum and Szkoła's distributions for the operators  $\rho_{AB}$  and  $\sigma_{AB}$ :

$$P_{\rho_{AB}, \sigma_{AB}}(r, b, a) = q_r |\langle u_r | b, \psi_a^b \rangle|^2, \quad (109a)$$

$$Q_{\rho_{AB}, \sigma_{AB}}(r, b, a) = P_{B,R}(b, a) |\langle u_r | b, \psi_a^b \rangle|^2. \quad (109b)$$

Since  $|\Psi\rangle_{ABR} = \sum_r \sqrt{q_r} |u_{AB}^r\rangle |v_r^r\rangle$ , it holds  $\langle v^r | \Psi \rangle \langle \Psi | v^r \rangle = q_r |u^r\rangle\langle u^r|$ . On the other hand, Eqs. (94) and (106) together imply that

$$|\psi\rangle_{ABR} = \sum_{b,a} \sqrt{p_{BR}(b,a)} |u^a|^b\rangle_A \otimes |b\rangle_B \otimes |v^a|^b\rangle_R. \quad (110)$$

This leads to

$$\begin{aligned} P_{\rho_{AB}, \sigma_{AB}}(r, b, a) \\ = q_r |\langle u_r | b, \psi_a^b \rangle|^2 \end{aligned} \quad (111)$$

$$= q_r \langle b, \psi_a^b | u_r \rangle \langle u_r | b, \psi_a^b \rangle \quad (112)$$

$$= \langle b, \psi_a^b | v_r \rangle \langle \psi | b, \psi_a^b | v_r \rangle \quad (113)$$

$$= \text{Tr}[(|b, \psi_a^b\rangle\langle b, \psi_a^b| \otimes \mathbb{1}_R) |\psi\rangle\langle \psi|] |\langle v_r | v_a^b \rangle|^2 \quad (114)$$

$$= P_{B,R}(b, a) |\langle v_a^b | v_r \rangle|^2 \quad (115)$$

$$= P_{\sigma_{BR}, \mathbb{1}_B \otimes \sigma_R}(b, a, r). \quad (116)$$

Hence we can check that

$$\begin{aligned} D_s^\varepsilon(P_{\sigma_{BR}, \mathbb{1}_B \otimes \sigma_R} \| Q_{\sigma_{BR}, \mathbb{1}_B \otimes \sigma_R}) \\ \stackrel{(a)}{=} \sup \{x : P_{\sigma_{BR}, \mathbb{1}_B \otimes \sigma_R}\{(b, a, r) | \\ \log P_{\sigma_{BR}, \mathbb{1}_B \otimes \sigma_R}(b, a, r) \\ - \log Q_{\sigma_{BR}, \mathbb{1}_B \otimes \sigma_R}(b, a, r) \leq x\} \leq \varepsilon\} \end{aligned} \quad (117)$$

$$\stackrel{(b)}{=} \sup \{x : P_{\sigma_{BR}, \mathbb{1}_B \otimes \sigma_R}\{(b, a, r) | \\ \log P_{B,R}(b, a) - \log q_r \leq x\} \leq \varepsilon\} \quad (118)$$

$$\stackrel{(c)}{=} \sup \{x : P_{\rho_{AB}, \Delta_B(\rho_{AB})}\{(b, a, r) | \\ \log P_{B,R}(b, a) - \log q_r \leq x\} \leq \varepsilon\} \quad (119)$$

$$\stackrel{(d)}{=} \sup \{x : P_{\rho_{AB}, \Delta_B(\rho_{AB})}\{(b, a, r) | \\ \log Q_{\rho, \Delta(\rho)}(b, a, r) \\ - \log P_{\rho, \Delta(\rho)}(b, a, r) \leq x\} \leq \varepsilon\} \quad (120)$$

$$\stackrel{(e)}{=} -D_s^{1-\varepsilon}(P_{\rho_{AB}, \Delta_B(\rho_{AB})} \| Q_{\rho_{AB}, \Delta_B(\rho_{AB})}), \quad (121)$$

where (a) and (e) follow by definition, (b) follows by (108), (c) follows by (116), and (d) follows by (109). This concludes (98). ■

*Proof of Eqs. (99) and (100):* We first show (99). Consider the following chain of equalities:

$$\begin{aligned} D(\sigma_{BR} \| \mathbb{1}_B \otimes \sigma_R) \\ \stackrel{(a)}{=} D(P_{\sigma_{BR}, \mathbb{1}_B \otimes \sigma_R} \| Q_{\sigma_{BR}, \mathbb{1}_B \otimes \sigma_R}) \end{aligned} \quad (122)$$

$$\stackrel{(b)}{=} \sum_{b,r} P_{\sigma_{BR}, \mathbb{1}_B \otimes \sigma_R}(b, r) [\log P_{\sigma_{BR}, \mathbb{1}_B \otimes \sigma_R}(b, r) \\ - \log Q_{\sigma_{BR}, \mathbb{1}_B \otimes \sigma_R}(b, r)] \quad (123)$$

$$\stackrel{(c)}{=} \sum_{b,r} P_{\rho_{AB}, \sigma_{AB}}(r, a) [\log p_a - \log q_r] \quad (124)$$

$$\stackrel{(d)}{=} \sum_{b,r} P_{\rho_{AB}, \sigma_{AB}}(r, a) [\log Q_{\rho_{AB}, \sigma_{AB}}(r, a) \\ - \log P_{\rho_{AB}, \sigma_{AB}}(r, a)] \quad (125)$$

$$\stackrel{(e)}{=} -D(P_{\rho_{AB}, \sigma_{AB}} \| Q_{\rho_{AB}, \sigma_{AB}}) \quad (126)$$

$$\stackrel{(f)}{=} -D(\rho_{AB} \| \sigma_{AB}), \quad (127)$$

where (a) and (f) follow from the property of Nussbaum and Szkoła's distributions (97), (b) and (e) follow by definition, (c) and (d) follow by (108), (109), (116). This completes the proof of (99). We can then prove (100) in a similar way. ■

*Proof of Eq. (101):* First notice that  $\sigma_R$  and  $\rho_{AB}$  are two marginal of the pure tripartite state  $\psi_{ABR}$ , thus they have the same eigenvalues. This gives  $\theta(\sigma_R) = \theta(\rho_{AB})$ . Consider the following chain of inequalities:

$$\begin{aligned} H_{\min}^\varepsilon(B|R)_\sigma \\ := -\inf_{\tau_R} D_{\max}^\varepsilon(\sigma_{BR} \| \mathbb{1}_B \otimes \tau_R) \end{aligned} \quad (128)$$

$$\geq -D_{\max}^\varepsilon(\sigma_{BR} \| \mathbb{1}_B \otimes \sigma_R) \quad (129)$$

$$\stackrel{(a)}{\geq} -D_s^{1-\varepsilon+\delta}(P_{\sigma_{BR}, \mathbb{1}_B \otimes \sigma_R} \| Q_{\sigma_{BR}, \mathbb{1}_B \otimes \sigma_R}) \\ - \log \theta(\rho_{AB}) + \log(\delta\varepsilon^2) \quad (130)$$

$$\stackrel{(b)}{=} D_s^{\varepsilon-2\delta}(P_{\rho_{AB}, \Delta(\rho_{AB})} \| Q_{\rho_{AB}, \Delta(\rho_{AB})}) \\ - \log \theta(\rho_{AB}) + \log(\delta\varepsilon^2) \quad (131)$$

$$\stackrel{(c)}{\geq} D_H^{\varepsilon^2 - 2\delta}(\rho_{AB} \| \Delta_B(\rho_{AB})) - c(\rho_{AB}, \varepsilon, \delta), \quad (132)$$

where (a) follows from [22, Eq. (29)] and the fact that  $\theta(\mathbb{1}_A \otimes \sigma_R) = \theta(\sigma_R) = \theta(\rho_{AB})$ , (b) follows from (98), and (c) follows from [22, Eq. (27)] with the correction term  $c(\rho_{AB}, \varepsilon, \delta)$  given in (102). Note that the constraints  $\delta < 1 - \varepsilon^2$  and  $\delta < \varepsilon^2/3$  are imposed in (a) and (c), respectively. This completes the proof. ■

## VII. CONCLUSION

Our work initiated the *first* systematic second order analysis on coherence distillation with and without assistance, filling an important gap in the literature. In the unassisted setting, we introduced a variant of randomness extraction framework in the context of quantum coherence theory, establishing an exact relation between this cryptographic task and the operational task of quantum coherence distillation. Based on this relation, we gave a finite block length analysis on these tasks, providing in particular explicit second order expansions of distillable coherence and extractable randomness under a diverse range of free operations. We then lifted the obtained results to the assisted setting in which Alice served as an assistant to help Bob do the manipulations. A crucial step for our second order expansions was the hypothesis testing characterizations of the one-shot rate with almost tight error dependence. These one-shot characterizations could be suitable for analysis even beyond the i.i.d. assumption of the source state if combining with a more refined result of hypothesis testing relative entropy (e.g., [70] and the references therein).

Many interesting problems remain open. First, in the unassisted setting the coincidence of the second order expansions of  $\ell_{\mathcal{O}}^{\varepsilon}$  and  $\ell_{\text{id}}^{\varepsilon}$  indicates that optimizing the free incoherent operations before the incoherent measurement can improve the extractable randomness by the order  $O(\log n)$  at most. One may explore whether there is any advantage of performing incoherent operations in the third or higher order terms. Second, as a reverse problem of coherence distillation, the coherence cost considers the minimum number of coherent bits required to prepare a quantum state. It is known that the first order asymptotics of coherence cost under IO operations is given by the coherence information [14]. But what is the second order expansion? Recall the critical role of the randomness extraction framework in our second order analysis. For coherence cost, we may consider a randomness extraction scenario with Eve having limited power. Such a scenario has been studied in [29] and [30, Section VI] and the corresponding randomness extraction rate happens to coincide with the coherence information. Finally, regarding the assisted scenario, it would be interesting to extend the exact one-shot relation between  $C_{a, \text{QIP}}^{\varepsilon}$  and  $\ell_{\text{QIP}}^{\varepsilon}$  to other free operation classes. It is also appealing to explore further the alternative formulation in Appendix B and identify achievable rate in terms of hypothesis testing relative entropy with  $\varepsilon$ -square error dependence.

### APPENDIX A

#### PROOF OF PROPOSITION 1

*Proof:* Let  $\sigma_R^*$  be a quantum state that attains the minimum in

$$d_{\text{sec}}(\rho[\text{id}, \Delta, f]_{LR} | R) = \min_{\sigma_R \in \mathcal{S}(R)} P(\rho[\text{id}, \Delta, f]_{LR}, \pi_L \otimes \sigma_R). \quad (A.133)$$

Let  $|\phi^*\rangle_{BR}$  on  $\mathcal{H}_B \otimes \mathcal{H}_R$  be a purification of  $\sigma_R^*$ . Thus we have

$$F(\rho[\text{id}, \Delta, f]_{LR}, \pi_L \otimes \sigma_R^*) \geq \sqrt{1 - \varepsilon^2}. \quad (A.134)$$

Define the incoherent isometry  $U_f$  from  $\mathcal{H}_B$  to  $\mathcal{H}_L \otimes \mathcal{H}_B$  as

$$U_f|b\rangle_B := |f(b)\rangle_L \otimes |b\rangle_B. \quad (A.135)$$

We choose normalized vectors  $|\phi_{\ell}\rangle_{BR}$  and normalization factors  $r_{\ell}$  such that

$$U_f|\psi\rangle_{BR} = \sum_{\ell \in \mathcal{L}} \sqrt{r_{\ell}} |\ell\rangle_L \otimes |\phi_{\ell}\rangle_{BR}, \quad (A.136)$$

$$\sqrt{r_{\ell}} |\phi_{\ell}\rangle_{BR} := \sum_{b \in \mathcal{B}: f(b)=\ell} \sqrt{p_b} |b\rangle_B \otimes |\psi_b\rangle_R. \quad (A.137)$$

By Uhlmann's theorem [66] there exists a unitary  $U_{\ell}$  on  $\mathcal{H}_B$  such that

$$\begin{aligned} F(\text{Tr}_B |\phi_{\ell}\rangle\langle\phi_{\ell}|_{BR}, \sigma_R^*) \\ = F(U_{\ell} |\phi_{\ell}\rangle_{BR}, |\phi^*\rangle_{BR}) = \langle\phi^* | U_{\ell} |\phi_{\ell}\rangle. \end{aligned} \quad (A.138)$$

Take  $U := \sum_{\ell \in \mathcal{L}} |\ell\rangle\langle\ell|_L \otimes U_{\ell}$ . We have

$$\begin{aligned} F(UU_f|\psi\rangle_{BR}, |\Psi_L\rangle \otimes |\phi^*\rangle_{BR}) \\ \stackrel{(a)}{=} F\left(\sum_{\ell \in \mathcal{L}} \sqrt{r_{\ell}} |\ell\rangle \otimes U_{\ell} |\phi_{\ell}\rangle, \sum_{\ell \in \mathcal{L}} \frac{1}{\sqrt{|\mathcal{L}|}} |\ell\rangle \otimes |\phi^*\rangle\right) \end{aligned} \quad (A.139)$$

$$\stackrel{(b)}{=} \sum_{\ell \in \mathcal{L}} \sqrt{r_{\ell}} \frac{1}{\sqrt{|\mathcal{L}|}} F(U_{\ell} |\phi_{\ell}\rangle, |\phi^*\rangle) \quad (A.140)$$

$$\stackrel{(c)}{=} \sum_{\ell \in \mathcal{L}} \sqrt{r_{\ell}} \frac{1}{\sqrt{|\mathcal{L}|}} F(\text{Tr}_B |\phi_{\ell}\rangle\langle\phi_{\ell}|, \sigma_R^*) \quad (A.141)$$

$$\stackrel{(d)}{=} F\left(\sum_{\ell \in \mathcal{L}} r_{\ell} |\ell\rangle\langle\ell| \otimes \text{Tr}_B |\phi_{\ell}\rangle\langle\phi_{\ell}|, \sum_{\ell \in \mathcal{L}} \frac{1}{|\mathcal{L}|} |\ell\rangle\langle\ell| \otimes \sigma_R^*\right) \quad (A.142)$$

$$\stackrel{(e)}{=} F(\rho[\text{id}, \Delta, f]_{LR}, \pi_L \otimes \sigma_R^*), \quad (A.143)$$

where (a) follows by definition, (b) and (d) follow from Lemma 3, (c) follows from Eq. (A.138) and (e) follows from the fact that  $\rho[\text{id}, \Delta, f]_{LR} = \sum_{\ell \in \mathcal{L}} r_{\ell} |\ell\rangle\langle\ell| \otimes \text{Tr}_B |\phi_{\ell}\rangle\langle\phi_{\ell}|$ . We construct a quantum operation  $\Gamma_{B \rightarrow L}(\cdot) := \text{Tr}_B[UU_f(\cdot)U_f^{\dagger}U^{\dagger}]$ , whose schematic diagram is given in Figure 5. Then  $\Gamma_{B \rightarrow L}(\rho_B) = \text{Tr}_{BR}[UU_f|\psi\rangle\langle\psi|_{BR}U_f^{\dagger}U^{\dagger}]$  and we can check that

$$\begin{aligned} F(\Gamma_{B \rightarrow L}(\rho_B), \Psi_L) \\ \geq F(UU_f|\psi\rangle_{BR}, |\Psi_L\rangle \otimes |\phi^*\rangle_{BR}) \end{aligned} \quad (A.144)$$

$$= F(\rho[\text{id}, \Delta, f]_{LR}, \pi_L \otimes \sigma_R^*) \quad (A.145)$$

$$\geq \sqrt{1 - \varepsilon^2}, \quad (A.146)$$

where the first inequality follows by the data-processing inequality of quantum fidelity under  $\text{Tr}_{BR}$ , the equality follows by (A.143) and the second inequality follows from (A.134). This implies that  $P(\Gamma_{B \rightarrow L}(\rho_B), \Psi_L) \leq \varepsilon$ .

It remains to check  $\Gamma \in \text{DIIO}$ . Note that  $\Gamma$  admits a Kraus decomposition  $\Gamma(\cdot) = \sum_{b \in \mathcal{B}} K_b U_f(\cdot) U_f^{\dagger} K_b^{\dagger}$  with operators  $K_b = \langle b | U$ . For any computational basis  $|x\rangle$  and any  $b \in \mathcal{B}$ , we have

$$K_b U_f |x\rangle \langle x| U_f^{\dagger} K_b^{\dagger} = |\langle b | U_{f(x)} |x\rangle|^2 |f(x)\rangle \langle f(x)| \in \mathcal{I}^{**}, \quad (A.147)$$

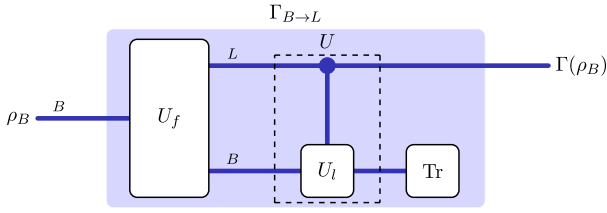


Fig. 5. Schematic diagram of the DIIO distillation protocol in Proposition 1. The isometry  $U_f$  is incoherent. The unitary  $U$ , represented by the inner dashed box, is a controlled unitary but is not necessarily incoherent. The overall operation  $\Gamma_{B \rightarrow L}$ , represented by the dashed box, belongs to DIIO.

by direct calculation. Thus  $\Gamma \in \text{IO}$ . For any computational basis  $|x\rangle$  and  $|y\rangle$ , we can first check that

$$\Gamma(|x\rangle\langle y|) = \langle y|U_{f(x)}^\dagger U_{f(y)}|x\rangle|f(x)\rangle\langle f(y)|. \quad (\text{A.148})$$

Thus it holds

$$\begin{aligned} \Gamma(\Delta(|x\rangle\langle y|)) &= \Gamma(\delta_{x,y}|x\rangle\langle x|) \\ &= \delta_{x,y}\Gamma(|x\rangle\langle x|) = \delta_{x,y}|f(x)\rangle\langle f(x)|, \end{aligned} \quad (\text{A.149})$$

and

$$\begin{aligned} \Delta(\Gamma(|x\rangle\langle y|)) &= \delta_{f(x),f(y)}\langle y|U_{f(x)}^\dagger U_{f(y)}|x\rangle|f(x)\rangle\langle f(x)| \\ &= \delta_{f(x),f(y)}\delta_{x,y}|f(x)\rangle\langle f(x)| \\ &= \delta_{x,y}|f(x)\rangle\langle f(x)|. \end{aligned} \quad (\text{A.150})$$

Combining (A.149) and (A.150), we have  $\Gamma \circ \Delta = \Delta \circ \Gamma$ , indicating that  $\Gamma \in \text{DIO}$ . Finally we have  $\Gamma \in \text{DIIO}$ . ■

## APPENDIX B

### AN ALTERNATIVE FORMULATION OF ASSISTED INCOHERENT RANDOMNESS EXTRACTION

In this appendix, we consider an alternative formulation of the assisted incoherent randomness extraction framework that is different from the one discussed in Section IV-C. In this formulation, Bob is more discreet in the sense that he accepts the assistance from Alice but does not allow her to possess any information about the extracted randomness.

#### A. Task Description

In the beginning, Alice and Bob share a bipartite quantum state  $\rho_{AB}$  with purification  $|\psi\rangle_{RAB}$  such that the reference system  $R$  held by Eve. A general assisted incoherent randomness extraction protocol is characterized by a triplet  $(\Lambda, \Delta, f)$ , where  $\Lambda \in \mathcal{F}$  a free operation and  $f$  a hash function. The protocol has three steps:

- 1) Alice and Bob first perform a free operation  $\Lambda_{AB \rightarrow C} \in \mathcal{F}$  on their joint system, where  $C$  is in Bob's possession. That is, there is no output system at Alice's hand anymore. This can be done by performing a partial trace operation. Let  $U_{AB \rightarrow CE}$  be a Stinespring isometry representation of  $\Lambda$ . We assume the environment system  $E$  of  $\Lambda$  is also controlled by Eve. After the action of  $\Lambda$ , the whole system is in a pure state

$$\tau[\Lambda]_{CER} := U_{AB \rightarrow CE}(|\psi\rangle\langle\psi|_{RAB})U_{AB \rightarrow CE}^\dagger, \quad (\text{B.151})$$

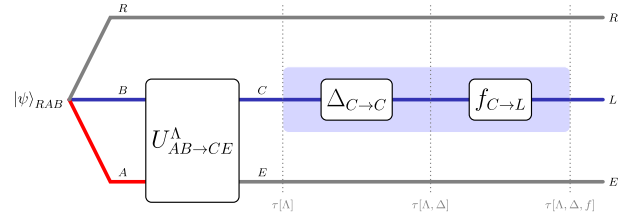


Fig. 6. Alternative formulation of the assisted randomness extraction framework given by  $[\Lambda, \Delta, f]$ . The system in red belongs to Alice, the system in blue belong to Bob, and the two systems in gray belong to Eve. In the shaded area, we illustrate an incoherent randomness extraction protocol  $[\text{id}, \Delta, f]$  (without assistance!) for the state  $\tau_C$  with purification  $\tau[\Lambda]_{CER}$ .

where we use  $\tau$  instead of  $\rho$  in (B.151) to indicate that we consider an alternative formulation here.

- 2) Bob dephases system  $C$  into the incoherent basis via  $\Delta_C$ .
- 3) Bob performs the hash function  $f$  to extract randomness. These two steps lead to the final output state

$$\begin{aligned} \tau[\Lambda, \Delta, f]_{LER} &:= \tau[\Lambda, \Delta]_{f(C)ER} \\ &= \sum_{b \in B} p_b |f(b)\rangle\langle f(b)|_L \otimes \sigma_{ER}^b, \end{aligned} \quad (\text{B.152})$$

where  $p_b := \text{Tr}\langle b|\tau[\Lambda]_{CER}|b\rangle$  and  $\sigma_{ER}^b := \langle b|\tau[\Lambda]_{CER}|b\rangle/p_b$ .

A detailed procedure of this alternative assisted randomness extraction via  $(\Lambda, \Delta, f)$  is depicted in Figure 6. Likewise, the *one-shot assisted extractable randomness* via  $\mathcal{F}$  of the quantum state  $\rho_{AB}$  in this alternative formulation is defined as

$$\begin{aligned} \tilde{\ell}_{\mathcal{F}}^{\varepsilon}(\rho_{AB}) &:= \max_{\Lambda_{AB \rightarrow C} \in \mathcal{F}} \max_f \{ \log |L| : \\ & d_{\text{sec}}(\tau[\Lambda, \Delta, f]_{LER}|ER) \leq \varepsilon \}. \end{aligned} \quad (\text{B.153})$$

*Remark 18:* As one can tell, the essential difference between this formulation and the original definition in Section IV-C lies in what kind of incoherent operation  $\Lambda \in \mathcal{F}$  that Alice and Bob can use. In the original definition, Alice and Bob can adopt operations of the form  $\Lambda_{AB \rightarrow A'B'}$  such that the output  $A'$  is at Alice's hand and  $B'$  is at Bob's hand. As a result, Alice has some information on Bob's extracted randomness that is secure from Eve. However, in this alternative formulation, we rule out this possibility by only allowing operations of the form  $\Lambda_{AB \rightarrow C}$  such that the output system  $C$  is under the full control of Bob. Apparently, Bob in the alternative formulation is more stringent since he solely makes use of Alice while does not allow her to possess any secrecy. However, this difference does not cause any trouble in the assisted coherence distillation scenario, since  $\Lambda_{AB \rightarrow A'B'}$  can be converted to  $\Lambda_{AB \rightarrow C}$  by doing an extra partial trace  $\text{Tr}_{A'}$  without affecting the distillation rate.

Based on the argument in Remark 18, we conclude that Bob in the original assisted randomness extraction framework (cf. Section IV-C) can extract more randomness than in this alternative framework.



*Proposition 5:* Let  $\mathcal{F} \in \{\text{LICC}, \text{LQICC}, \text{SI}, \text{SQI}, \text{QIP}\}$ . Let  $\rho_{AB}$  be a bipartite quantum state and  $\varepsilon \in [0, 1]$ . It holds that

$$\tilde{\ell}_{\mathcal{F}}^{\varepsilon}(\rho_{AB}) \leq \ell_{\mathcal{F}}^{\varepsilon}(\rho_{AB}). \quad (\text{B.154})$$

### B. New Equivalence Relation

The main advantage of this alternative assisted incoherent randomness extraction framework is that we can establish an equivalence relation between the assisted coherence distillation described in Section IV-B and the alternative assisted incoherent randomness extraction described here, for all free operation classes under consideration. This equivalence hence is much stronger than that was concluded in Theorem 3, holding only for the QIP class.

*Theorem 6 (Equivalence Relation II):* Let  $\mathcal{F} \in \{\text{LICC}, \text{LQICC}, \text{SI}, \text{SQI}, \text{QIP}\}$ . Let  $\rho_{AB}$  be a bipartite quantum state and  $\varepsilon \in [0, 1]$ . It holds that

$$C_{d,\mathcal{F}}^{\varepsilon}(\rho_{AB}) = \tilde{\ell}_{\mathcal{F}}^{\varepsilon}(\rho_{AB}). \quad (\text{B.155})$$

*Proof:* “ $\leq$ ”: This direction can be shown using similar argument in Lemma 1.

“ $\geq$ ”: Let  $\ell_{\mathcal{F}}^{\varepsilon}(\rho_{AB}) = \log |L|$  and let  $[\Lambda, \Delta, f]$  achieves this rate such that  $\Lambda_{AB \rightarrow C} \in \mathcal{F}$ . The key observation is that an assisted incoherent randomness extraction protocol  $[\Lambda_{AB \rightarrow C}, \Delta_C, f]$  for state  $\rho_{AB}$  can be regarded as an incoherent randomness extraction protocol  $[\text{id}_{C \rightarrow C}, \Delta_C, f]$  (without assistance) for the state  $\tau_C \equiv \Lambda_{AB \rightarrow C}(\rho_{AB})$ , with purification  $\tau[\Lambda]_{CER}$  defined in (B.151) and joint reference system  $ER$  (cf. the shaded area of Figure 6). That is, for the state  $\tau_C$ , there exists a hash function  $f$  such that

$$d_{\text{sec}}(\tau[\text{id}, \Delta, f]_{LER}|ER) \leq \varepsilon. \quad (\text{B.156})$$

Recalling the one-to-one correspondence between coherence distillation protocol and incoherent randomness extraction protocol in Proposition 1, we conclude from (B.156) that there exists a quantum operation  $\Gamma_{C \rightarrow L} \in \text{DIIO}$  such that  $P(\Gamma_{C \rightarrow L}(\tau_C), \Psi_L) \leq \varepsilon$ . Compositing these two quantum operations yields

$$\begin{aligned} & P(\Gamma_{C \rightarrow L}(\tau_C), \Psi_L) \\ &= P(\Gamma_{C \rightarrow L} \circ \Lambda_{AB \rightarrow C}(\rho_{AB}), \Psi_L) \leq \varepsilon. \end{aligned} \quad (\text{B.157})$$

That is to say, the composite operation  $\Gamma \circ \Lambda$  distills an MCS of rank  $|L|$  such that the error is bounded by  $\varepsilon$ . It then suffices to show that  $\Gamma \circ \Lambda \in \mathcal{F}$ . In the following, we handle case by case to show that the conditions  $\Lambda \in \mathcal{F}$  and  $\Gamma \in \text{DIIO}$  together indeed imply that  $\Gamma \circ \Lambda \in \mathcal{F}$ .

*Cases that  $\mathcal{F} \equiv \text{LICC}$  or  $\mathcal{F} \equiv \text{LQICC}$ .* We only consider  $\mathcal{F} \equiv \text{LQICC}$  since the other case  $\mathcal{F} \equiv \text{LICC}$  can be shown similarly. We focus on the last round of classical communication in the local incoherent operations and classical communication operation  $\Lambda_{AB \rightarrow C} \in \text{LQICC}$ . It must be that Bob sends her outcome to Bob. More specifically, in the last round, Bob performs a POVM  $\{E_A^x\}$  such that  $E_A^x \geq 0$  and  $\sum_x E_A^x = \mathbb{1}$ . She sends the outcome  $x$  to Bob. Conditioned on  $x$ , Bob performs an operation  $\mathcal{D}_{B \rightarrow C}^x \in \text{MIO}$  on the post-measurement state. After that, he continues to do the operation  $\Gamma_{C \rightarrow L}$ . Since  $\Gamma_{C \rightarrow L} \in \text{DIIO}$ , we know  $\Gamma \circ \mathcal{D}^x \in \text{MIO}$  as

$\text{DIIO} \subseteq \text{MIO}$  and  $\text{MIO}$  is closed under composition. As one can tell, the only difference between  $\Lambda$  and  $\Gamma \circ \Lambda$  is that in the last round Bob performs different conditional operations; for the former  $\mathcal{D}^x$  is taken, while for the latter  $\Gamma \circ \mathcal{D}^x$  is adopted. They are both free local incoherent operations. Hence,  $\Gamma \circ \Lambda \in \text{LQICC}$ .

*Cases that  $\mathcal{F} \equiv \text{SI}$  or  $\mathcal{F} \equiv \text{SQI}$ .* We only consider  $\mathcal{F} \equiv \text{SI}$  since the other case  $\mathcal{F} \equiv \text{SQI}$  can be shown similarly. Assume the incoherent operations  $\Lambda_{AB \rightarrow C} \in \text{SI}$  has the form

$$\Lambda_{AB \rightarrow C}(\cdot) = \sum_i (A_i \otimes B_i)(\cdot)(A_i \otimes B_i)^\dagger, \quad (\text{B.158})$$

where both  $A_i$  and  $B_i$  are incoherent Kraus operators. Since  $\text{DIIO} \subset \text{IO}$ ,  $\Gamma_{C \rightarrow L}$  admits an incoherent Kraus decomposition as  $\Gamma_{C \rightarrow L}(\rho) = \sum_l K_l \rho K_l^\dagger$ , where  $K_l$  are incoherent Kraus operators. Thus,  $\Gamma \circ \Lambda$  admits the decomposition

$$\begin{aligned} & \Gamma_{C \rightarrow L} \circ \Lambda_{AB \rightarrow C}(\rho_{AB}) \\ &= \sum_l K_l \left( \sum_i (A_i \otimes B_i) \rho_{AB} (A_i \otimes B_i)^\dagger \right) K_l^\dagger \end{aligned} \quad (\text{B.159})$$

$$= \sum_{l,i} (A_i \otimes K_l B_i) \rho_{AB} (A_i \otimes K_l B_i)^\dagger. \quad (\text{B.160})$$

The completeness condition holds since

$$\begin{aligned} & \sum_{l,i} (A_i \otimes K_l B_i)^\dagger (A_i \otimes K_l B_i) \\ &= \sum_i (A_i \otimes B_i)^\dagger \left( \sum_l K_l^\dagger K_l \right) (A_i \otimes B_i) \end{aligned} \quad (\text{B.161})$$

$$= \sum_i (A_i \otimes B_i)^\dagger (A_i \otimes B_i) = \mathbb{1}_{AB}. \quad (\text{B.162})$$

What’s more, the Kraus operators  $K_l B_i$  are incoherent since incoherent Kraus operators are closed under composition. Hence  $\Gamma \circ \Lambda \in \text{SI}$ .

*Cases that  $\mathcal{F} \equiv \text{QIP}$ .* Notice that  $\text{DIIO}$  preserves the free incoherent states  $\mathcal{I}$ . On the other hand it holds by definition that  $\mathcal{I} \subset \mathcal{QT}$ . Thus  $\text{DIIO}$  preserves  $\mathcal{QT}$ . This implies that  $\Gamma(\mathcal{QT}) \subset \mathcal{QT}$ . Since  $\Lambda \in \text{QIP}$  and  $\text{QIP}$  is closed under composition, we conclude  $\Gamma \circ \Lambda \in \text{QIP}$ . ■

### C. Comparison Among Various Assisted Tasks

We have considered three assisted tasks concerning a bipartite quantum state  $\rho_{AB}$  in this work:

- 1) The assisted coherence distillation task introduced in Section IV-B and the corresponding one-shot optimal rate  $C_{d,\mathcal{F}}^{\varepsilon}(\rho_{AB})$  (31),
- 2) The assisted incoherent randomness extraction task introduced in Section IV-C and the corresponding one-shot optimal rate  $\ell_{\mathcal{F}}^{\varepsilon}(\rho_{AB})$  (38), and
- 3) An alternative formulation of the assisted incoherent randomness extraction task introduced in Appendix B and the corresponding one-shot optimal rate  $\tilde{\ell}_{\mathcal{F}}^{\varepsilon}(\rho_{AB})$  (B.153).

The following relation holds among these quantities as a consequence of Proposition 5 and Theorem 6:

$$C_{d,\mathcal{F}}^{\varepsilon}(\rho_{AB}) = \tilde{\ell}_{\mathcal{F}}^{\varepsilon}(\rho_{AB}) \leq \ell_{\mathcal{F}}^{\varepsilon}(\rho_{AB}). \quad (\text{B.163})$$

Specially, for the class of QIP we obtain an equivalence relation due to Theorem 3 and Theorem 6:

$$C_{d,\text{QIP}}^{\varepsilon}(\rho_{AB}) = \tilde{\ell}_{\text{QIP}}^{\varepsilon}(\rho_{AB}) = \ell_{\text{QIP}}^{\varepsilon}(\rho_{AB}). \quad (\text{B.164})$$

To prove or disprove that the inequality in (B.163) is an equality for other free classes is left to future work.

#### ACKNOWLEDGMENT

The authors would like to Anurag Anshu and Xin Wang for discussions about the second order expansion of distillable coherence. Masahito Hayashi and Kun Fang would like to thank the Center for Quantum Computing at Peng Cheng Laboratory for their hospitality while part of this work was done during their visit.

#### REFERENCES

- [1] E. Chitambar and G. Gour, "Quantum resource theories," *Rev. Modern Phys.*, vol. 91, no. 2, Apr. 2019, Art. no. 025001.
- [2] A. Streltsov, G. Adesso, and M. B. Plenio, "Quantum coherence as a resource," *Rev. Modern Phys.*, vol. 89, no. 4, 2017, Art. no. 041003.
- [3] M. Hillery, "Coherence as a resource in decision problems: The Deutsch-Jozsa algorithm and a variation," *Phys. Rev. A, Gen. Phys.*, vol. 93, no. 1, 2016, Art. no. 012111.
- [4] P. J. Coles, E. M. Metodiev, and N. Lütkenhaus, "Numerical approach for unstructured quantum key distribution," *Nature Commun.*, vol. 7, no. 1, 2016, Art. no. 11712.
- [5] A. Streltsov, E. Chitambar, S. Rana, M. Bera, A. Winter, and M. Lewenstein, "Entanglement and coherence in quantum state merging," *Phys. Rev. Lett.*, vol. 116, Jun. 2016, Art. no. 240405.
- [6] A. Anshu, R. Jain, and A. Streltsov, "Quantum state redistribution with local coherence," 2018, *arXiv:1804.04915*. [Online]. Available: <http://arxiv.org/abs/1804.04915>
- [7] M. G. Díaz *et al.*, "Using and reusing coherence to realize quantum processes," *Quantum*, vol. 2, p. 100, Oct. 2018, doi: [10.22331/q-2018-10-19-100](https://doi.org/10.22331/q-2018-10-19-100).
- [8] M. Lostaglio, D. Jennings, and T. Rudolph, "Description of quantum coherence in thermodynamic processes requires constraints beyond free energy," *Nature Commun.*, vol. 6, p. 6383, 2015.
- [9] F. Fröwis and W. Dür, "Stable macroscopic quantum superpositions," *Phys. Rev. Lett.*, vol. 106, no. 11, Mar. 2011, Art. no. 110402. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.106.110402>
- [10] J. Aberg, "Quantifying superposition," 2006, *arXiv:quant-ph/0612146*. [Online]. Available: <https://arxiv.org/abs/quant-ph/0612146>
- [11] G. Gour and R. W. Spekkens, "The resource theory of quantum reference frames: Manipulations and monotones," *New J. Phys.*, vol. 10, no. 3, 2008, Art. no. 033023.
- [12] F. Levi and F. Mintert, "A quantitative theory of coherent delocalization," *New J. Phys.*, vol. 16, no. 3, 2014, Art. no. 033007.
- [13] T. Baumgratz, M. Cramer, and M. B. Plenio, "Quantifying coherence," *Phys. Rev. Lett.*, vol. 113, no. 14, 2014, Art. no. 140401.
- [14] A. Winter and D. Yang, "Operational resource theory of coherence," *Phys. Rev. Lett.*, vol. 116, Mar. 2016, Art. no. 120404.
- [15] E. Chitambar, A. Streltsov, S. Rana, M. Bera, G. Adesso, and M. Lewenstein, "Assisted distillation of quantum coherence," *Phys. Rev. Lett.*, vol. 116, no. 7, 2016, Art. no. 070402.
- [16] E. Chitambar and M.-H. Hsieh, "Relating the resource theories of entanglement and quantum coherence," *Phys. Rev. Lett.*, vol. 117, Jul. 2016, Art. no. 020402.
- [17] B. Regula, K. Fang, X. Wang, and G. Adesso, "One-shot coherence distillation," *Phys. Rev. Lett.*, vol. 121, no. 1, 2018, Art. no. 010401.
- [18] K. Fang, X. Wang, L. Lami, B. Regula, and G. Adesso, "Probabilistic distillation of quantum coherence," *Phys. Rev. Lett.*, vol. 121, no. 7, Aug. 2018, Art. no. 070404.
- [19] Q. Zhao, Y. Liu, X. Yuan, E. Chitambar, and X. Ma, "One-shot coherence dilution," *Phys. Rev. Lett.*, vol. 120, no. 7, Feb. 2018, Art. no. 070403.
- [20] L. Lami, "Completing the grand tour of asymptotic quantum coherence manipulation," *IEEE Trans. Inf. Theory*, vol. 66, no. 4, pp. 2165–2183, Apr. 2020.
- [21] M. Hayashi, "Second-order asymptotics in fixed-length source coding and intrinsic randomness," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4619–4637, Oct. 2008.
- [22] M. Tomamichel and M. Hayashi, "A hierarchy of information quantities for finite block length analysis of quantum tasks," *IEEE Trans. Inf. Theory*, vol. 59, no. 11, pp. 7693–7710, Nov. 2013.
- [23] K. Li, "Second-order asymptotics for quantum hypothesis testing," *Ann. Statist.*, vol. 42, no. 1, pp. 171–189, Feb. 2014.
- [24] N. Datta and F. Leditzky, "Second-order asymptotics for source coding, dense coding, and pure-state entanglement conversions," *IEEE Trans. Inf. Theory*, vol. 61, no. 1, pp. 582–608, Jan. 2015.
- [25] M. Tomamichel, M. Berta, and J. M. Renes, "Quantum coding with finite resources," *Nature Commun.*, vol. 7, no. 1, pp. 1–8, Sep. 2016.
- [26] K. Fang, X. Wang, M. Tomamichel, and R. Duan, "Non-asymptotic entanglement distillation," *IEEE Trans. Inf. Theory*, vol. 65, no. 10, pp. 6454–6465, Oct. 2019.
- [27] X. Wang, K. Fang, and M. Tomamichel, "On converse bounds for classical communication over quantum channels," *IEEE Trans. Inf. Theory*, vol. 65, no. 7, pp. 4609–4619, Jul. 2019.
- [28] Q. Zhao, Y. Liu, X. Yuan, E. Chitambar, and A. Winter, "One-shot coherence distillation: Towards completing the picture," *IEEE Trans. Inf. Theory*, vol. 65, no. 10, pp. 6441–6453, Oct. 2019.
- [29] X. Yuan, H. Zhou, Z. Cao, and X. Ma, "Intrinsic randomness as a measure of quantum coherence," *Phys. Rev. A, Gen. Phys.*, vol. 92, no. 2, Aug. 2015, Art. no. 022124.
- [30] M. Hayashi and H. Zhu, "Secure uniform random-number extraction via incoherent strategies," *Phys. Rev. A, Gen. Phys.*, vol. 97, no. 1, Jan. 2018, Art. no. 012302.
- [31] D. P. DiVincenzo, C. A. Fuchs, H. Mabuchi, J. A. Smolin, A. Thapliyal, and A. Uhlmann, "Entanglement of assistance," in *Proc. NASA Int. Conf. Quantum Comput. Quantum Commun.* Berlin, Germany: Springer, 1998, pp. 247–257.
- [32] M. Gregoratti and R. F. Werner, "Quantum lost and found," *J. Modern Opt.*, vol. 50, nos. 6–7, pp. 915–933, Apr. 2003.
- [33] P. Hayden and C. King, "Correcting quantum channels by measuring the environment," 2004, *arXiv:quant-ph/0409026*. [Online]. Available: <https://arxiv.org/abs/quant-ph/0409026>
- [34] J. A. Smolin, F. Verstraete, and A. Winter, "Entanglement of assistance and multipartite state distillation," *Phys. Rev. A, Gen. Phys.*, vol. 72, no. 5, Nov. 2005, Art. no. 052317.
- [35] A. Winter, "On environment-assisted capacities of quantum channels," 2005, *arXiv:quant-ph/0507045*. [Online]. Available: <https://arxiv.org/abs/quant-ph/0507045>
- [36] F. Buscemi, G. Chiribella, and G. Mauro D'Ariano, "Inverting quantum decoherence by classical feedback from the environment," *Phys. Rev. Lett.*, vol. 95, no. 9, Aug. 2005, Art. no. 090501.
- [37] F. Buscemi, "Channel correction via quantum erasure," *Phys. Rev. Lett.*, vol. 99, no. 18, Oct. 2007, Art. no. 180501.
- [38] N. Dutil and P. Hayden, "Assisted entanglement distillation," 2010, *arXiv:1011.1972*. [Online]. Available: <http://arxiv.org/abs/1011.1972>
- [39] F. Buscemi and N. Datta, "General theory of environment-assisted entanglement distillation," *IEEE Trans. Inf. Theory*, vol. 59, no. 3, pp. 1940–1954, Mar. 2013.
- [40] S. Karumanchi, S. Mancini, A. Winter, and D. Yang, "Classical capacities of quantum channels with environment assistance," *Problems Inf. Transmiss.*, vol. 52, no. 3, pp. 214–238, Jul. 2016.
- [41] S. Karumanchi, S. Mancini, A. Winter, and D. Yang, "Quantum channel capacities with passive environment assistance," *IEEE Trans. Inf. Theory*, vol. 62, no. 4, pp. 1733–1747, Apr. 2016.
- [42] L. Lami, R. Takagi, and G. Adesso, "Assisted concentration of Gaussian resources," *Phys. Rev. A, Gen. Phys.*, vol. 101, no. 5, May 2020, Art. no. 052305.
- [43] A. Streltsov, S. Rana, M. N. Bera, and M. Lewenstein, "Towards resource theory of coherence in distributed scenarios," *Phys. Rev. X*, vol. 7, no. 1, Mar. 2017, Art. no. 011024.
- [44] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, "Quantum entanglement," *Rev. Modern Phys.*, vol. 81, p. 865, Jun. 2009.
- [45] M.-J. Zhao, T. Ma, and S.-M. Fei, "Coherence of assistance and regularized coherence of assistance," *Phys. Rev. A, Gen. Phys.*, vol. 96, no. 6, Dec. 2017, Art. no. 062332.
- [46] M.-J. Zhao, T. Ma, Q. Quan, H. Fan, and R. Pereira, "L<sub>1</sub>-norm coherence of assistance," *Phys. Rev. A, Gen. Phys.*, vol. 100, no. 1, Jul. 2019, Art. no. 012315.
- [47] K.-D. Wu *et al.*, "Experimentally obtaining maximal coherence via assisted distillation process," *Optica*, vol. 4, no. 4, pp. 454–459, 2017.
- [48] K.-D. Wu *et al.*, "Experimental cyclic interconversion between coherence and quantum correlations," *Phys. Rev. Lett.*, vol. 121, no. 5, Aug. 2018, Art. no. 050401.

- [49] K.-D. Wu *et al.*, “Quantum coherence and state conversion: Theory and experiment,” *NPJ Quantum Inf.*, vol. 6, no. 1, pp. 1–9, Dec. 2020.
- [50] B. Regula, L. Lami, and A. Streltsov, “Nonasymptotic assisted distillation of quantum coherence,” *Phys. Rev. A, Gen. Phys.*, vol. 98, no. 5, Nov. 2018, Art. no. 052329.
- [51] M. K. Vijayan, E. Chitambar, and M.-H. Hsieh, “One-shot assisted concentration of coherence,” *J. Phys. A, Math. Theor.*, vol. 51, no. 41, Oct. 2018, Art. no. 414001.
- [52] M. Tomamichel, *Quantum Information Processing With Finite Resources: Mathematical Foundations*, vol. 5. Heidelberg, Germany: Springer, 2015.
- [53] F. Buscemi and N. Datta, “The quantum capacity of channels with arbitrarily correlated noise,” *IEEE Trans. Inf. Theory*, vol. 56, no. 3, pp. 1447–1460, Mar. 2010.
- [54] F. G. S. L. Brandao and N. Datta, “One-shot rates for entanglement manipulation under non-entangling maps,” *IEEE Trans. Inf. Theory*, vol. 57, no. 3, pp. 1754–1760, Mar. 2011.
- [55] L. Wang and R. Renner, “One-shot classical-quantum capacity and hypothesis testing,” *Phys. Rev. Lett.*, vol. 108, no. 20, May 2012, Art. no. 200501.
- [56] N. Datta, “Min- and max-relative entropies and a new entanglement monotone,” *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2816–2826, Jun. 2009.
- [57] E. Chitambar and G. Gour, “Critical examination of incoherent operations and a physically consistent resource theory of quantum coherence,” *Phys. Rev. Lett.*, vol. 117, no. 3, Jul. 2016, Art. no. 030401.
- [58] I. Marvian and R. W. Spekkens, “How to quantify coherence: Distinguishing speakable and unspeakable notions,” *Phys. Rev. A, Gen. Phys.*, vol. 94, no. 5, Nov. 2016, Art. no. 052324.
- [59] J. I. de Vicente and A. Streltsov, “Genuine quantum coherence,” *J. Phys. A, Math. Theor.*, vol. 50, no. 4, Jan. 2017, Art. no. 045301.
- [60] L. Lami, B. Regula, and G. Adesso, “Generic bound coherence under strictly incoherent operations,” *Phys. Rev. Lett.*, vol. 122, no. 15, Apr. 2019, Art. no. 150402.
- [61] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, “Tight finite-key analysis for quantum cryptography,” *Nature Commun.*, vol. 3, no. 1, pp. 1–6, Jan. 2012.
- [62] P. W. Shor and J. Preskill, “Simple proof of security of the bb84 quantum key distribution protocol,” *Phys. Rev. Lett.*, vol. 85, no. 2, p. 441, 2000.
- [63] M. Hayashi, “Practical evaluation of security for quantum key distribution,” *Phys. Rev. A, Gen. Phys.*, vol. 74, no. 2, Aug. 2006, Art. no. 022307.
- [64] K. Li, A. Winter, X. Zou, and G. Guo, “Private capacity of quantum channels is not additive,” *Phys. Rev. Lett.*, vol. 103, no. 12, Sep. 2009, Art. no. 120501.
- [65] R. Renner, “Security of quantum key distribution,” Ph.D. dissertation, ETH Zürich, Zürich, Switzerland, Dec. 2005. [Online]. Available: <http://arxiv.org/abs/quant-ph/0512258>
- [66] A. Uhlmann, “The ‘transition probability’ in the state space of \*-algebra,” *Rep. Math. Phys.*, vol. 9, no. 2, pp. 273–279, 1976.
- [67] H. Yamasaki, M. K. Vijayan, and M.-H. Hsieh, “Hierarchy of quantum operations in manipulating coherence and entanglement,” 2019, *arXiv:1912.11049*. [Online]. Available: <http://arxiv.org/abs/1912.11049>
- [68] D. Yang, K. Horodecki, and A. Winter, “Distributed private randomness distillation,” *Phys. Rev. Lett.*, vol. 123, no. 17, Oct. 2019, Art. no. 170501.
- [69] M. Nussbaum and A. Szkoła, “The Chernoff lower bound for symmetric quantum hypothesis testing,” *Ann. Statist.*, vol. 37, no. 2, pp. 1040–1057, Apr. 2009.
- [70] N. Datta, Y. Pautrat, and C. Rouzé, “Second-order asymptotics for quantum hypothesis testing in settings beyond iid—Quantum lattice systems and more,” *J. Math. Phys.*, vol. 57, no. 6, 2016, Art. no. 062207.

**Masahito Hayashi** (Fellow, IEEE) was born in Japan, in 1971. He received the B.S. degree from the Faculty of Sciences, Kyoto University, Japan, in 1994, and the M.S. and Ph.D. degrees in mathematics from Kyoto University, Japan, in 1996 and 1999, respectively. He worked with Kyoto University as a Research Fellow of the Japan Society of the Promotion of Science (JSPS) from 1998 to 2000; the Laboratory for Mathematical Neuroscience, Brain Science Institute, RIKEN, from 2000 to 2003; the ERATO Quantum Computation and Information Project, Japan Science and Technology Agency (JST), as the Research Head, from 2000 to 2006; the Superrobust Computation Project Information Science and Technology Strategic Core (21st Century COE by MEXT), Graduate School of Information Science and Technology, The University of Tokyo, as an Adjunct Associate Professor, from 2004 to 2007; and the Graduate School of Information Sciences, Tohoku University, as an Associate Professor, from 2007 to 2012. In 2012, he joined the Graduate School of Mathematics, Nagoya University, as a Professor. He was appointed as a Visiting Research Associate Professor at the Centre for Quantum Technologies, National University of Singapore, from 2009 to 2012, where he was a Visiting Research Professor since 2012. He worked at the Center for Advanced Intelligence Project, RIKEN, as a Visiting Scientist, from 2017 to 2020. He worked at the Shenzhen Institute for Quantum Science and Engineering, Southern University of Science and Technology, Shenzhen, China, as a Visiting Professor, from 2018 to 2020, and the Center for Quantum Computing, Peng Cheng Laboratory, Shenzhen, as a Visiting Professor, from 2019 to 2020. In 2020, he joined the Shenzhen Institute for Quantum Science and Engineering, Southern University of Science and Technology, Shenzhen, as a Chief Research Scientist. He has published the book *Quantum Information: An Introduction* (Springer, 2006), whose revised version was published as *Quantum Information Theory: Mathematical Foundation From Graduate Texts in Physics* (Springer, 2016). He has also published other two books *Group Representation for Quantum Theory and A Group Theoretic Approach to Quantum Information* (Springer, 2016). His research interests include classical and quantum information theory and classical and quantum statistical inference. He is on the Editorial Board of the *International Journal of Quantum Information* and *International Journal on Advances in Security*. He received the Information Theory Society Paper Award for “Information-Spectrum Approach to Second-Order Coding Rate in Channel Coding” in 2011 and the Japan Academy Medal from the Japan Academy and the JSPS Prize from Japan Society for the Promotion of Science in 2016.

**Kun Fang** received the B.S. degree from Wuhan University, and the Ph.D. degree in quantum information from the University of Technology Sydney, in October 2018. He was a Post-Doctoral Researcher with the Department of Applied Mathematics and Theoretical Physics, University of Cambridge, and the Institute for Quantum Computing, University of Waterloo. He is currently a Research Scientist with the Institute for Quantum Computing, Baidu Research. His research interests include quantum information theory and optimization theory.

**Kun Wang** received the Ph.D. degree in quantum information from Nanjing University in 2019. He was a Post-Doctoral Researcher with the Shenzhen Institute for Quantum Science and Engineering, Southern University of Science and Technology. He is currently a Research Scientist with the Institute for Quantum Computing, Baidu Research. His research interests include quantum information theory and the applications of majorization theory.